Revista Brasileira de Direito Processual Penal

Volume 5 - Nº 03 - set./dez. 2019
ISSN 2525-510X
https://doi.org/10.22197/rbdpp.v5i3

Dossiê "Novas Tecnologias e Processo Penal"

IBRASPP

Revista Brasileira de Direito Processual Penal
Brazilian Journal of Criminal Procedure
http://www.ibraspp.com.br/revista/
ISSN 2525-510X

Volume 5 - Número 03
Porto Alegre/RS
set./dez. 2019
(publicado em outubro/2019)

Expediente / Masthead

Autores de artigos originais (deste número) / Authors of original articles (in this number)

Alexandre Rocha Almeida de Moraes (Pontifícia Universidade Católica de São Paulo – São Paulo/SP)

Chiara Gabrielli (Università degli Studi di Urbino Carlo Bo – Italia)

Daniele Negri (Università degli Studi di Ferrara – Italia)

Delia Magherescu (Gorj Bar Association – Romania)

Fabio Alonzi (Università degli Studi di ROMA "La Sapienza" – Italia)

Flávio da Silva Andrade (Universidade Federal de Minas Gerais - Belo Horizonte/MG)

Gianluca Martins Smanio (Universidade de São Paulo – São Paulo/SP)

Gustavo Mascarenhas Lacerda Pedrina (Universidade de São Paulo – São Paulo/SP)

Jacqueline de Souza Abreu (Universidade de São Paulo – São Paulo/SP)

Luís Greco (Universidade Humboldt - Berlim, Alemanha)

Mª Isabel González Cano (Universidad de Sevilla – España)

Marcello Daniele (Università degli Studi di Padova - Italia)

Miren Josune Pérez Estrada (Universidad del País Vasco – España)

Orlandino Gleizer (Universidade Humboldt - Berlim, Alemanha)

Pablo García Molina (Universidad de Cádiz – Cádiz/España)

Rafael de Oliveira Costa (Ministério Público do Estado de São Paulo – São Paulo/SP)

Rodrigo Régnier Chemim Guimarães (Universidade Positivo - Curitiba/Paraná)

Serena Quattrocolo (University of Eastern Piedmont – Italy)

Projeto Gráfico [Diagramação e Capa] Camila Provenzi (be.net/camilaprovenzi)

Sumário
Table of contents

Nota del gruppo editoriale della RBDPP in ricordo di Mª Isabel González Cano (1º aprile 1965 – 20 ottobre 2019)

Nelle more della pubblicazione, la prof.ssa Mª Isabel González Cano si è improvvisamente spenta a Braga durante un breve viaggio di lavoro. La sua prematura scomparsa ha commosso numerosi amici e colleghi. E per tutto l'impegno che aveva profuso a favore della ricerca e dell'insegnamento, eravamo in tanti a stimarla e non possiamo non ricordarla con gratitudine.

Cattedratica di Diritto Processuale presso la Facoltà di Giurisprudenza dell'Università di Siviglia da gennaio 2010, si è dottorata nel 1993 all'Università Carlos III di Madrid *Summa cum laude*, vincendo in seguito il premio straordinario per la sua tesi di dottorato.

Per noi, tuttavia, ricordare Isabel González è opera a dir poco improba. Quelle che per prime affollano la nostra mente sono le infinite sfumature emotive che appartengono alla quotidianità del rapporto che intercorre fra amici o nelle relazioni umane di successo: un apprezzamento o un rimprovero, una vigile critica, l'allegria di un pranzo o di una cena, un messaggio all'ultimo minuto per chiedere un consiglio, un istante di complicità, un sorriso o uno sguardo di incoraggiamento in un momento difficile.

Nondimeno, se l'ufficialità ci costringe ad uscire da questa dimensione più intima – che pure è preponderante – e si deve provare a condensare in fretta e in pochissime righe la memoria della prof.ssa González, è allora necessario rintracciare qualcuna delle linee guida che hanno caratterizzato, nella formalità accademica, la sua personalità.

L'attività scientifica della prof.ssa González ha riguardato molteplici settori del Diritto Processuale e la González ha preso parte con serena, positiva e sorridente autorevolezza a numerosi progetti di ricerca di rilevanza nazionale, europea e internazionale: *El sistema de impugnación de las resoluciones judiciales en el derecho español*, diretto dal prof. Victor Moreno Catena (cod. Otri 00453, ref. Pb-95-0293); *Aspectos delictuales de investigación y enjuiciamiento criminal en materia de*

delincuencia organizada, finanziato dalla commissione europea nell'ambito del programma Falcone (progetto Falcone 99/FAL/167); ecc. ecc.

Negli oltre vent'anni di carriera presso l'Università di Siviglia, Isabel González ha svolto una ricca attività didattica, che ha sempre coinvolto ed entusiasmato gli studenti e i giovani ricercatori: ha tenuto lezioni nell'ambito dei corsi di Diritto Processuale I e II, Diritto Processuale Civile, Diritto Processuale Penale, Diritto Processuale del Lavoro, Diritto dell'esecuzione penale, soltanto per citarne alcuni.

La prof.ssa González ha ricoperto inoltre numerosi e prestigiosi incarichi istituzionali. Da ultimo, era membro permanente della commissione generale spagnola di codificazione di Diritto Processuale; vicepresidente dell'Associazione dei professori di Diritto processuale delle Università spagnole – APDPUE; vicepresidente per la Spagna e il Portogallo dell'Istituto iberoamericano di Diritto processuale – IIDP; membro dell'Associazione internazionale di Diritto Processuale – IAPL.

Seppur nella consapevolezza che non sarebbe possibile ricordare adeguatamente in questa sede le cariche occupate e i riconoscimenti ricevuti nella sua lunga, prestigiosa carriera, e che ciascuno di noi ha avuto con la prof.ssa González un rapporto culturale e personale diverso, abbiamo ritenuto comunque essere questo un momento di sintesi appropriato per omaggiare Isabel González per quello che è stata davvero, e che sarà sempre nel nostro ricordo: una maestra di scienza e di vita, una persona misurata negli apprezzamenti e nelle critiche, studiosa illuminata. Un esempio di equilibrio, tenacia, sensibilità, correttezza e rigore per tutti coloro che hanno avuto il privilegio di incontrarla. Una persona presente, attenta, discreta, capace di dimostrare sempre un intenso interessamento per il prossimo.

La prof.ssa González lascia in tutti noi un grande vuoto umano e scientifico.

A lei, per parte nostra, è dedicato il presente fascicolo.

Il gruppo editoriale della RBDPP

Nota del equipo editorial del RBDPP en memoria de Mª Isabel González Cano (1 de abril de 1965 - 20 de octubre de 2019)

En el transcurso de la publicación, la profesora Mª Isabel González Cano falleció repentinamente en Braga durante un corto viaje de trabajo. Su fallecimiento prematuro ha conmocionado a muchos amigos y colegas. Y por todos los esfuerzos que había hecho a favor de la investigación y de la enseñanza, somos muchos los que la estimamos y no podemos dejar de recordarla con gratitud.

Catedrática de Derecho Procesal en la Facultad de Derecho de la Universidad de Sevilla desde enero de 2010, obtuvo su doctorado en 1993 por la Universidad Carlos III de Madrid *Summa cum laude*, y posteriormente ganó el premio extraordinario por su tesis doctoral.

Para nosotros, todavía, recordar a Isabel González es una ardua tarea. Lo primero que se nos viene a la mente son los infinitos matices emocionales que pertenecen a la relación cotidiana entre amigos o a las relaciones humanas más prósperas: una apreciación o un reproche, una crítica, la alegría de un almuerzo o una cena, un mensaje en el último minuto para pedir un consejo, un momento de complicidad, una sonrisa o una mirada de aliento en un momento difícil.

No obstante, si la formalidad nos obliga a abandonar esta dimensión más íntima – que no deja de ser predominante – y debemos intentar resumir rápidamente y en pocas líneas el recuerdo de la profesora González, entonces es necesario señalar algunas de las pautas que han caracterizado, en el ámbito académico, su personalidad.

La actividad científica de la profesora ha cubierto múltiples áreas del Derecho Procesal, donde ha participado con autoridad serena, positiva y sonriente en numerosos proyectos de investigación de relevancia nacional, europea e internacional: *El sistema de impugnación de las resoluciones judiciales en el derecho español*, dirigido por el prof. Victor Moreno Catena (cod. Otri 00453, ref. Pb-95-0293); *Aspectos delictuales de investigación y enjuiciamiento criminal en materia de delincuencia organizada*, financiado

por la Comisión europea en el ámbito del programa Falcone (proyecto Falcone 99/FAL/167), etc. etc.

En más de veinte años de carrera en la Universidad de Sevilla, Isabel González ha llevado a cabo una rica actividad docente, que siempre ha involucrado y entusiasmado a estudiantes y jóvenes investigadores: ha impartido clases en los cursos de Derecho Procesal I y II, Derecho Procesal Civil, Derecho Procesal Penal, Derecho Procesal Laboral, Ejecución Penal, por nombrar solo algunos.

La profesora González también ha ocupado numerosos puestos institucionales de prestigio. Recientemente, era miembro permanente de la Comisión General de Codificación Española; vicepresidente de la Asociación de Profesores de Derecho Procesal de las Universidades Españolas - APDPUE; vicepresidente por España y Portugal del Instituto Iberoamericano de Derecho Procesal - IIDP; miembro de la Asociación Internacional de Derecho Procesal - IAPL.

A sabiendas de que no sería posible recordar aquí, de forma adecuada, todos los puestos ocupados y los premios recibidos en su larga y prestigiosa carrera, y de que cada uno de nosotros tenía una relación cultural y personal diferente con la profesora González, hemos estimado oportuno, en este momento de síntesis, rendir homenaje a Isabel González por lo que realmente era, y que siempre estará en nuestra memoria: una maestra de ciencia y vida, una persona comedida en las apreciaciones y en las críticas, una estudiosa iluminada. Un ejemplo de equilibrio, tenacidad, sensibilidad, equidad y rigor para todos aquellos que han tenido el privilegio de conocerla. Una persona presente, atenta, discreta, capaz de mostrar siempre un gran interés por los demás.

La profesora González deja un gran vacío humano y científico en todos nosotros.

A ella, le dedicamos este número de RBDPP.

El equipo editorial de la RBDPP

Nota da equipe editorial da RBDPP em memória à Mª Isabel González Cano (1º de abril de 1965 – 20 de outubro de 2019)

Durante a espera pela publicação, a prof. Mª Isabel González Cano abruptamente faleceu em Braga durante uma breve viagem de trabalho. O seu prematuro falecimento comoveu numerosos amigos e colegas. E por todo o empenho que havia dedicado em prol da pesquisa e do ensino, éramos em muitos a admirá-la e não podemos deixar de recorda-la com gratidão.

Catedrática de Direito Processual pela Faculdade de Direito da Universidade de Sevilha desde janeiro de 2010, se doutorou em 1993 pela Universidade Carlos III de Madri *Summa cum laude*, vencendo em seguida o prêmio extraordinário por sua tese de doutorado.

Para nós, todavia, recordar Isabel González é uma tarefa tortuosa. Aquilo que primeiramente surge em nossas mentes são as infinitas nuanças emotivas que pertencem ao quotidiano de uma relação entre amigos ou que intercorrem nas relações humanas de sucesso: um elogio ou uma repreensão, uma crítica vigilante, a alegria de um almoço ou de um jantar, uma mensagem de última hora para pedir conselhos, um momento de cumplicidade, um sorriso ou um olhar de encorajamento em um momento difícil.

No entanto, se a oficialidade nos obriga a deixar essa dimensão mais íntima – que de qualquer forma é predominante – e devemos tentar condensar às pressas e em poucas linhas a memória da professora González, é necessário traçar alguns esboços que caracterizaram, na formalidade acadêmica, sua personalidade.

A atividade científica da professora González envolveu várias áreas do Direito Processual, em que participou com serena, positiva e sorridente autoridade em inúmeros projetos de pesquisa de relevância nacional, europeia e internacional: *El sistema de impugnación de las resoluciones judiciales en el derecho español*, dirigido pelo prof. Victor Moreno Catena (cod. Otri 00453, ref. Pb-95-0293); *Aspectos delictuales de investigación y enjuiciamiento criminal en materia de delincuencia organizada*, financiado

pela comissão europeia no âmbito do programa Falcone (projeto Falcone 99/FAL/167); etc. etc.

Em mais de vinte anos de carreira na Universidade de Sevilha, Isabel González realizou uma rica atividade de ensino, envolvendo e cativando sempre seus alunos e jovens pesquisadores: lecionou nos cursos de Direito Processual I e II, Direito Processual Civil, Direito Processual Penal, Direito Processual Trabalhista, Execução Penal, somente para citar alguns exemplos.

A professora González também ocupou vários cargos institucionais de prestígio. Ultimamente, era membro permanente da comissão geral de codificação espanhola; vice-presidente da Associação de Professores de Direito Processual das Universidades Espanholas – APDPUE; vice-presidente para Espanha e Portugal do Instituto Ibero-americano de Direito Processual – IIDP; membro da Associação Internacional de Direito Processual – IAPL.

Embora se tenha consciência que não seria possível recordar adequadamente aqui os cargos ocupados e os prêmios recebidos em sua longa e prestigiada carreira, e que cada um de nós teve uma relação cultural e pessoal diferente com a professora González, consideramos que este seja um momento de síntese apropriada para homenagear Isabel González pelo que ela realmente era, e que sempre sará em nossa memória: mestre de ciência e de vida, ponderada na apreciação e na crítica, professora iluminada. Um exemplo de equilíbrio, tenacidade, sensibilidade, exatidão e rigor para todos aqueles que tiveram o privilégio de conhecê-la. Uma pessoa presente, atenciosa, discreta, capaz de mostrar sempre um intenso interesse pelos outros.

A professora González nos deixa um grande vazio humano e científico.

A ela, por nós, é dedicado o presente número da RBDPP.

Equipe Editorial da RBDPP

Un piccolo ringraziamento dalla RBDPP

Sono passati esattamente quattro anni da quando, nel 2015 a Porto Alegre, un ristretto gruppo di ragazzi appassionati di ricerca decisero di dedicare il proprio tempo e le proprie energie al progetto editoriale della *Revista Brasileira de Direito Processual Penal*. Un progetto nato senza troppe pretese, in un clima di grande collaborazione, condivisione e appassionata complicità, che ci ha permesso di iniziare una serie di attività per il consolidamento della *Revista*, creando uno spazio di libertà e crescita culturale nel panorama scientifico, in cui non si discute solo di scienza, ma anche del nostro futuro. Ciò ancor più nei tempi della delicata mutazione del sistema universitario in corso, la quale ci impone di recepire le istanze di pluralismo e trasversalità proprie della ricerca, e di coniugarle con i canoni tipici della valutazione scientifica (originalità, appropriatezza del metodo, dimostrata consapevolezza dello stato dell'arte, ecc. ecc.), all'interno di un contesto storico, culturale e istituzionale in costante trasformazione, caratterizzato da accelerazioni spesso disomogenee, le cui ragioni antropologiche paiono relegate a un passato troppo lontano e si dimostrano incapaci di giudicare il presente.

Ma sin dagli esordi la RBDPP non voleva essere l'ennesima rivista scientifica, bensì un ponte tra la nostra disciplina e altre aree culturali; un periodico piacevole da leggere e che desse spazio al pensiero indipendente e alla creatività, che avvicinasse le diverse tradizioni processuali e che ci aiutasse a riscoprire le nostre radici.

A partire dal 2017 – a seguito di innumerevoli ristrutturazioni del periodico, che già allora iniziava a darci i primi riscontri positivi –, con il sostegno e la proficua collaborazione di numerosi e autorevoli professori italiani, spagnoli, portoghesi, inglesi, latinoamericani, brasiliani e di altre parti del globo abbiamo adottato importanti misure per colmare le lacune preesistenti, apportando diversi miglioramenti sia alle nostre politiche editoriali, sia alle questioni di integrità scientifica, che all'internazionalizzazione della rivista. Invero, siamo attualmente indicizzati nei principali database bibliografico-citazionali multidisciplinari di periodici scientifici, unendo in questo modo la possibilità di effettuare

ricerche tematiche sia per autore, sia per le citazioni che un determinato autore o un determinato contributo ottengono in un arco di tempo definito: Emerging Sources Citation Index (WoS), Scopus, DOAJ, Dialnet, Latindex, Google Scholar (h 5 5; mediana h 5 7), ecc. ecc., divenendo così veicolo di promozione e identità scientifica e sostenendo l'internazionalizzazione dei nostri Autori e dei nostri Revisori.

Negli ultimi tre numeri della rivista (vol. 4 num. 3, vol. 5 num. 1 e vol. 5 num. 2), sono stati pubblicati quarantuno contributi originali, oltre a cinque editoriali a contenuto scientifico.

Sempre nell'arco temporale appena indicato (vol. 4 num. 3, vol. 5 num. 1 e vol. 5 num. 2), rispetto ai cinquantotto Autori che ci hanno generosamente offerto la propria collaborazione, trentadue di essi possiedono un vincolo con un'istituzione di insegnamento estera (nel 60% dei casi, detta istituzione è europea).

E ancora con riferimento ai tre volumi precedenti al fascicolo in corso (vol. 4 num. 3, vol. 5 num. 1 e vol. 5 num. 2), facciamo notare che, rispetto ai primi anni di attività della RBDPP (2015, 2016, 2017), il numero dei Revisori vincolati a Università straniere è aumento esponenzialmente: dei centoquattro *Reviewers* menzionati nei fascicoli di riferimento, sessanta di essi appartengono a Università estere (nel 69% dei casi a Università europee).

E per assicurare ai Lettori e ai Ricercatori la qualità del volume, anche nel 2019 la *Revista* ha continuato ad aumentare il rigore della selezione dei saggi proposti per la pubblicazione, suscitando in questo modo ampi consensi nella comunità scientifica.

Altrettanto può dirsi per l'uscita dei numeri monografici, la cui periodicità quadrimestrale va diffondendo il nome e il prestigio della RBDPP in maniera ancor più capillare. Contemporaneamente, si sono superate alcune restrizioni editoriali, vincenti nel passato ma ormai obsolete, che avrebbero limitato il maggior sviluppo della RBDPP. Del resto, fin dal gennaio del 2017 si è deciso di pubblicare nei fascicoli ordinari sia saggi in lingua italiana, sia nelle altre lingue ufficiali della rivista (inglese, spagnolo e portoghese).

Nondimeno, ai fini della valutazione dei prodotti scientifici, da qualche mese la RBDPP figura tra le riviste straniere cui l'Anvur assegna

la patente di scientificità, oltre a essere accreditata come un periodico di classe A nella collocazione in fascia.

A distanza di quattro anni, dunque, ci conforta guardare indietro e vedere come siamo riusciti a concretizzare molti – se non tutti – gli obiettivi entro il termine che ci siamo posti. Un'esperienza editoriale difficile ed entusiasmante, ma premiata da un successo che ci gratifica enormemente. E ci è d'obbligo condividerlo con Voi e ringraziarVi per quanto fatto fino a qui.

Ora, però, non ci resta che pensare al lavoro che abbiamo davanti, e, con l'auspicio che questo sia soltanto l'inizio di una duratura e fruttuosa collaborazione, i nostri ringraziamenti più sinceri e affettuosi vanno dunque ai Curatori dei nostri dossier, agli Autori, ai Revisori, ai Lettori, agli Editori, ai membri del nostro comitato scientifico e a ogni altro nostro "sostenitore e/o seguace", per averci accolto e salutato con favore, per la fondamentale opera svolta in questi quattro anni in seno alla RBDPP, e per averci dato la possibilità di crescere e di partecipare a un'avventura così intensa e affascinante.

Bologna-Porto Alegre, ottobre 2019.

Bruna Capparelli
Vinicius Gomes de Vasconcellos
Nereu José Giacomolli

Um breve agradecimento da equipe editorial da RBDPP

Passados quatro anos desde quando, em 2015 na cidade de Porto Alegre, um pequeno grupo de pesquisadores apaixonados pela pesquisa decidiram dedicar tempo e energia no projeto editorial da Revista Brasileira de Direito Processual Penal. Tratou-se de um projeto nascido sem maiores pretensões, em um clima de grande colaboração, cumplicidade e amigável cumplicidade, que permitiu o início de uma série de atividades para a consolidação do periódico, criando um espaço de liberdade e crescimento cultural no panorama científico, em que não se discute somente ciência, mas também o nosso futuro.

Isso se ressalta diante do cenário de delicadas mudanças no sistema universitário atual, com a crescente importância do pluralismo e da interdisciplinaridade da própria pesquisa, e diante da sua conjugação com as premissas típicas do pensamento científico (originalidade, adequação do método, consistente conhecimento do estado da arte, etc.), considerando um contexto histórico, cultural e institucional em constante transformação, caracterizado pela aceleração até não homogênea, cujas razões antropológicas restam relegadas a um passado longínquo e incapazes de analisar o presente.

Contudo, a RBDPP não pretendia ser mais uma revista científica, mas uma ponte entre a nossa disciplina e outras áreas do conhecimento; um periódico de agradável leitura e que assegurasse espaço para o pensamento independente e a criatividade, que aproximasse as diversas tradições processuais e que ajudasse a redescobrir a nossa origem. Para tanto, desde sempre pretendeu-se abrir espaço a novas pesquisas de pesquisadores já consolidados, mas também teses inovadoras e consistentes de jovens cientistas, com carreiras em consolidação.

A partir de 2017 – como decorrência de diversas reestruturações do periódico, especialmente a partir de uma base sólidas de premissas de editoração científica, que já naquele momento começavam a gerar resultados positivos –, com substanciais e profícuas contribuições de numerosos e destacados professores italianos, espanhóis, portugueses, ingleses, latino-americanos, brasileiros e de outras partes do mundo, a RBDPP adotou

importantes medidas para preencher a lacuna preexistente, aportando diversos aprimoramentos tanto nas suas políticas editoriais, quanto em termos de integridade científica e de internacionalização dos debates.

Atualmente, a RBDPP está indexadas em inúmeros dos mais importantes sistemas internacionais, possibilitando pesquisas temáticas e por autor ou a verificação do impacto das produções pelo número de citações: Emerging Sources Citation Index (WoS), Scopus, DOAJ, Dialnet, Latindex, Google Scholar (h 5 5; mediana h 5 7), etc., tornando-se assim instrumento de promoção e identidade científica e sustentando a internacionalização dos seus autores e pareceristas (esses por meio de inovadora parceria com o sistema Publons).

Nos últimos três números da revista (V4N3, V5N1 e V5N2), em relação aos cinquenta e oito autores que generosamente contribuíram com as suas pesquisas, trinta e dois possuem vínculo com instituição de ensino estrangeira ao Brasil (em 60% dos casos, com vínculo europeu).

Ainda em relação a tais números anteriores, pode-se destacar que, comparativamente aos três primeiros anos de atividade da RBDPP (2015-2017), o número de revisores vinculados a universidades estrangeiras aumentou exponencialmente: dos cento e quatro pareceristas atuantes, sessenta pertencem a universidades estrangeiras (em 69% dos casos, europeias).

E para assegurar aos leitores e pesquisadores a qualidade dos números, em 2019 a RBDPP tem continuado aumentar o rigor na seleção dos artigos e o sistema de controle por pares com o objetivo de aportar cada vez mais contribuições nas rodadas de correções, possibilitando, assim, crescente reconhecimento na comunidade científica.

Desse modo, a publicação dos números da revista e dos dossiês temáticos na periodicidade quadrimestral tem contribuído para difundir o nome e o prestígio da RBDPP de modo cada vez mais consistente. Desde janeiro de 2017, ampliou-se a abrangência do periódico com a publicação de artigos em italiano, inglês, espanhol e português.

Diante disso, ao fim da avaliação das produções científicas, recentemente a RBDPP passou a figurar entre as revistas estrangeiras a que Anvur (órgão oficial de avaliação científica italiano) certifica a cientificidade, qualificada como um periódico de estrato A, nota máxima em seu ramo.

Depois de quatro anos, com alegria percebe-se a obtenção dos objetivos anteriormente traçados e o reconhecimento do trabalho realizado pela equipe editorial. Sem dúvidas, trata-se de um projeto científico complexo e entusiasmante, mas recompensado com resultados que devem ser agradecidos intensamente. E, por óbvio, isso deve ser dividido com vocês, leitores e pesquisadores (autores, revisores e editores) a quem se deve agradecer muito por tudo realizado.

Agora, entretanto, é necessário pensar sobre as tarefas pendentes em frente e, com a dedicação que caracteriza esta duradoura e frutífera colaboração, os nossos agradecimentos dirigem-se especialmente aos Editores-associados que coordenaram dossiês temáticos, autores, pareceristas, editores, leitores, membros do conselho editorial e a todos que incentivaram e torceram pelo sucesso do projeto, por toda a confiança e gentil dedicação, que marcaram a história da RBDPP nesses quatro anos, e pela oportunidade de crescimento e de participação em meio a uma aventura tão intensa e fascinante.

Bolonha-Porto Alegre, outubro de 2019.

Bruna Capparelli
Vinicius Gomes de Vasconcellos
Nereu José Giacomolli

Dossiê:
Novas Tecnologias e Processo Penal

New technologies and criminal procedure

Editoriale: L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite

Editorial: The impact of new Technologies on criminal justice – an horizon with unknown implications

Editorial: O impacto das novas tecnologias sobre a justiça penal – um horizonte denso de incógnitas

Claudia Cesari[1]

Università degli Studi di Macerata/Italia

claudia.cesari@libero.it

https://orcid.org/0000-0002-1022-3086

Abstract: La società contemporanea è dominata dalle nuove tecnologie, connotate da un'evoluzione rapidissima e da una capacità espansiva immane, in tutti gli ambiti della vita individuale e collettiva. Anche nell'area del procedimento penale l'uso di strumenti tecnologici avanzati muta significativamente la fisionomia del sistema, con un impatto evidente sulle pratiche, ma anche su diritti, garanzie, istituti-chiave. Il contributo propone una panoramica delle aree in cui questo fenomeno è più evidente e delle principali implicazioni che ha, nella prospettiva della tutela dei principi cardine del sistema processuale e dei diritti fondamentali del singolo.

Parole chiave: nuove tecnologie e procedimento penale; giustizia predittiva; intelligenza artificiale; prova digitale; sorveglianza elettronica.

Abstract: *Modern society is dominated by new technologies, which have a quick expansion and a dramatic expansive attitude, in every area of individual and collective life. In the field of criminal proceedings, too, the use of advanced technological tools changes significantly the features of the system, with a visible*

[1] Professore Ordinario di Diritto Processuale Penale – Università degli Studi di Macerata. *Associate editor* RBDPP, volume 5 numero 3/2019.

impact on practices, but also on rights, safeguards and basic rules. This essay proposes a view of the areas of criminal justice where this phenomenon is more evident and of the main implications it has, in the perspective of protection of the basic principles of criminal proceedings and of fundamental rights of individuals.

Keywords: *new technologies and criminal proceedings; predictive justice; artificial intelligence; digital evidence; electronic monitoring.*

Resumo: *A sociedade contemporânea é dominada pelas novas tecnologias, marcadas por uma rapidíssima evolução e por uma capacidade expansiva inerente, em todos os âmbitos da vida individual e coletiva. Até mesmo no âmbito do processo penal o uso de instrumentos tecnológicos avançados modifica significativamente a fisionomia do sistema, com um impacto evidente em relação às práticas, direitos, garantias, institutos-chave. Este editorial apresenta um panorama dos tópicos da justiça criminal em que esse fenômeno é mais evidente e acarreta suas principais implicações, na perspectiva da tutela dos princípios essenciais do sistema processual e dos direitos fundamentais do individuo.*

Palavras-chave: *novas tecnologias e processo penal; justiça preditiva; inteligência artificial; prova digital; vigilância eletrônica.*

1. Evoluzione tecnologica e processo penale: il panorama complessivo

Che la società stia attraversando, a livello globale, un momento di sviluppo inedito e rapidissimo sul piano dell'elaborazione e dell'impiego di strumenti tecnologici innovativi ed avanzati, in tutti i campi della vita individuale e collettiva, oggi è solo una constatazione. Il grado di penetrazione di questo arsenale tecnologico inedito nell'esistenza quotidiana dei singoli e delle collettività è tale, da rendere ormai impensabile il farne a meno e da porlo come componente ineludibile – tanto pervasiva, che ne siamo talora inconsapevoli – di ogni area della

vita sociale. La giustizia penale e, in seno ad essa, il processo penale, non fanno eccezione.

Anche una mera elencazione degli ambiti applicativi attuali delle nuove tecnologie nell'area del procedimento penale non potrebbe che peccare di incompletezza e – pur a voler pensare che fosse allo stato esaustiva – sarebbe destinata a diventare obsoleta nel volgere di pochi mesi. Senza dire di quanto il panorama si amplierebbe, se si volessero enunciare non gli usi che si fanno ora delle nuove tecnologie nel rito penale, ma le potenzialità d'uso che gli sviluppi vorticosi della ricerca in questo campo potrebbero fornire molto presto.

Volendo offrire almeno una panoramica a grandi linee delle aree del sistema maggiormente interessate all'impatto dell'evoluzione tecnologica nel sistema processuale penale, si nota a colpo d'occhio che pressoché ogni settore di esso ne è toccato, benché in modi diversi e con maggiore o minore intensità. L'area delle prove penali è quella che subito viene in mente, giacché è il settore delle cosiddette *digital evidence* e *automated evidence*[2] ad avere acquisito sempre maggior rilievo nella prassi quotidiana della giustizia penale: si pensi a perquisizioni e sequestri su documenti informatici, all'apprensione processuale di e-mail o sms, fino alle captazioni effettuate direttamente tramite virus informatici installati sui *devices* dell'intercettato. A ben guardare, però, si può andare ben oltre questi confini, e constatare fino a che punto il sistema stia subendo una specie di "torsione tecnologica" con la quale si devono fare i conti in maniera organica. La verbalizzazione per mezzo di audiovisivi offre forme di costituzione, conservazione e riproduzione della memoria processuale con elevati gradi di affidabilità ed efficienza. La

[2] Le definizioni alludono qui, la prima, a ogni forma di raccolta ed impiego procedimentali di «dati originariamente contenuti in supporti informatici o telematici, oppure ancora trasmessi in modalità digitale» (M Pittiruti, *Digital evidence e procedimento penale*, Giappichelli, 2017, p. 8); la seconda, all' «impiego processuale di dati conoscitivi che siano trattati e generati automaticamente, attraverso algoritmi», più o meno sofisticati (S. Quattrocolo, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Italo-Espanola de derecho procesal*, 2019, p. 3). Va detto che le due definizioni possono anche sovrapporsi e che comunque le categorie definitorie in quest'ambito si prestano a numerose ricostruzioni e sottodistinzioni piuttosto complesse: cfr. A. Testaguzza, Digital forensics. *Informatica giuridica e processo penale*, Cedam, 2015, p. 2 ss.

possibilità di celebrare udienze a distanza, mediante tecnologie digitali[3] che assicurano la possibilità di collegare in remoto persino più di due luoghi contemporaneamente, fornisce lo strumentario per evitare i trasferimenti di imputati da un luogo all'altro e consente di razionalizzare tempi e costi dello svolgimento dei giudizi in procedimenti complessi o con imputati ad alto rischio, impattando direttamente con il modo di intendere la dialettica processuale[4] e la stessa nozione di "udienza". Le tecnologie della sorveglianza elettronica (oggi legate all'elaborazione continua di mezzi di controllo agili, leggeri, efficienti e con potenzialità intrusive mai conosciute prima) permettono di controllare a distanza gli spostamenti di indagati e imputati con un impiego minimo di personale di polizia e potenzialmente su aree territoriali sconfinate: si pensi solo al tracciamento mediante dispositivi di geolocalizzazione (*GPS tracking*)[5]. Persino il campo della decisione giudiziale – che si direbbe ineludibilmente legato all'esclusiva gestione umana – è investito dalla possibilità (attuale in alcuni ordinamenti) di spendere a fini decisori i risultati degli "algoritmi predittivi", ossia di strumenti di previsione del rischio su basi statistiche gestiti da appositi programmi, in grado di prevedere il pericolo di recidiva

---

[3] Sulla transizione alle tecnologie digitali anche di quest'area del sistema, v. M. Daniele, *La formazione digitale delle prove dichiarative*, Giappichelli, 2012, p. 7 ss.

[4] Sulla compatibilità di questa soluzione con l'art. 111 comma 4 Cost., trattandosi di una forma di contraddittorio attenuato, ma non negato, v. M. Daniele, *La sagomatura dell'esame a distanza nel perimetro del contraddittorio*, in D. Negri, R. Orlandi (a cura di), *Le erosioni silenziose al contraddittorio,* Giappichelli, 2017, p. 133. In generale, sul progressivo ampliarsi dell'area della "giustizia penale elettronica", v. S. Buzzelli, *Le modifiche alla disciplina della partecipazione a distanza*, in L. Giuliani, R. Orlandi (a cura di), *Indagini preliminari e giudizio di primo grado*, Giappichelli, 2018, p. 73 ss.

[5] Il tema ha sollevato un dibattito intenso in Italia, con riferimento al tipo di aggressione ai diritti individuali che l'uso del mezzo – dapprima tipicamente finalizzato al "pedinamento elettronico" dell'indagato ad opera della polizia giudiziaria - comporta, alle relative difficoltà di armonizzazione con il dettato costituzionale e alla conseguente costruzione delle garanzie processuali: per una compiuta ricostruzione, con le relative indicazioni bibliografiche, v. G. Di Paolo, *"Tecnologie del controllo" e prova penale*, Cedam, 2008, p. 251 ss.; A. Serrani, *Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie*, in *Arch. pen.* (web), 2013, n. 3

o di fuga in capo all'imputato, rilevanti ai fini di svariati provvedimenti, sia durante il procedimento penale che al suo esito[6].

2. I VANTAGGI

E' indubbio che la tecnologia possa offrire alla giustizia penale strumenti a vario livello vantaggiosi. Al di là del fatto che il procedimento penale è specchio della società in cui vive, sicché se oggi questa si fonda su un arsenale tecnologico in continua espansione ed evoluzione, è impossibile che esso ne prescinda, si deve ammettere che gli strumenti tecnologici più sofisticati offrono al sistema un ampio novero di potenziali benefici.

Innanzitutto, in vari ambiti l'impiego della tecnologia garantisce livelli di efficacia senza precedenti. E' intuitivo, ad esempio, come l'attitudine intrusiva del captatore informatico (un *malicious software* definito comunemente "virus *Trojan horse*" e installabile su un apparecchio portatile) comporti un aumento esponenziale delle informazioni intercettabili per suo tramite, sia per la qualità dei dati captabili, sia per la capacità di seguire ovunque il possessore dello strumento opportunamente "infettato" [7], in modo da creare un'intercettazione

---

[6] Cfr. M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *www.dirittopenalecontemporaneo.it*, 29 maggio 2019, p.3. L'Autore sottolinea come questi strumenti facciano parte di un arsenale vario, che ricomprende anche le prove digitali, l'*automated evidence* e la *e-evidence*, ascrivibile alla più ampia categoria dell'intelligenza artificiale utilizzata nel processo penale.

[7] Per tutti, da ultimo, F. Caprioli, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *questa Rivista*, 2017, n. 3, p. 483 ss.; P.P. Rivello, *Le intercettazioni mediante captatore informatico*, in O. Mazza (a cura di), *Le nuove intercettazioni*, Giappichelli, 2018, p. 102 ss.; per la medesima constatazione a livello giurisprudenziale, Cass., sez. un., 28 aprile 2016, Scurato, in *Arch. nuova proc. pen.*, 2017, p. 91, con nota di A. Camon, *Cavalli di Troia in Cassazione*. Nel sistema italiano lo strumento ha trovato una disciplina di riferimento solo di recente, con il d.lgs. 29 dicembre 2017, n. 216, che ha modificato *in parte qua* la disciplina delle intercettazioni (art. 266 ss. C.p.p.): per un primo commento, v. P. Bronzo, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in G. Giostra, R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni*, Giappichelli, 2018, p. 235 ss.; S. Signorato, *Modalità procedimentali dell'intercettazione tramite captatore informatico*, *ibidem*, p. 263 ss.

ubiquitaria e polifunzionale, capace di offrire al processo un'enorme mole di informazioni e dati, non comparabile a quella che si poteva trarre dalla tradizionale "intercettazione telefonica". Emblematico, in questa prospettiva, anche lo sviluppo applicativo delle "tecnologie del controllo" in ambito penale: è palese che la sorveglianza di un indagato sottoposto agli arresti domiciliari è lacunosa e debole se condotta utilizzando il personale di polizia direttamente sul posto (tramite piantonamento o verifiche "a sorpresa"), ma estremamente efficace se effettuata con il "braccialetto elettronico", che assicura una sorveglianza continuativa della permanenza in casa dell'indagato[8]. Senza dire che la tecnologia offre in concreto le uniche efficaci modalità di controllo del rispetto di misure specifiche, come i *restraining orders* a protezione della vittima, di nuovo conio in ordinamenti come quello italiano, in cui infatti hanno imposto l'uso della geolocalizzazione[9].

A queste potenzialità si aggiungono sovente considerevoli vantaggi in termini di efficienza, ossia di miglioramento del rapporto costi-benefici in diversi ambiti. Utilizzare lo strumentario tecnologico nel rito penale, infatti, garantisce oggi un significativo risparmio di risorse, che nasce da due profili distinti. Da un lato, la tecnologia è sempre più diffusa ed accessibile, anche economicamente, assicurando la presenza sul mercato di prodotti assai avanzati a costi bassi o comunque ragionevoli, che ne favoriscono l'impiego anche da parte di un sistema pubblico dal bilancio sofferente. Dall'altro, l'uso della tecnologia può avere un impatto positivo sui costi del processo, riducendoli anche in misura rilevante. Di nuovo, il pensiero corre all'uso della telematica: attraverso la celebrazione a distanza delle udienze, ad esempio, si possono evitare non solo i rischi, ma anche i costi del trasferimento degli imputati dal luogo di detenzione alla sede di svolgimento del giudizio. Lo stesso è a dirsi della sorveglianza elettronica, utile a garantire il miglior controllo sul territorio di soggetti sottoposti a

---

[8] Sulle ragioni che sempre stanno dietro all'adozione di sistemi di sorveglianza elettronica e sulla centralità in seno ad esse di logiche di incremento del controllo penale (spesso per soddisfare il bisogno di sicurezza della pubblica opinione) cfr. L. Cesaris, *Dal* panopticon *alla sorveglianza elettronica*, in M.Bargis (a cura di*), Il decreto "antiscarcerazioni"*, Giappichelli, 2001, p. 51 ss.

[9] V. *infra*, D. Negri, *Nuove tecnologie e compressione della libertà personale: la sorveglianza con dispositivi elettronici dell'imputato sottoposto a misure cautelari*.

misure custodiali, così ponendosi come efficace supporto alla riduzione del sovraffollamento carcerario[10], che impone spese di mantenimento spropositate della popolazione detenuta, oltre a comportare condizioni inumane di espiazione della pena.

Infine, i potenziali benefici si espandono ad ambiti che fino a poco tempo fa sarebbero stati considerati a dir poco fantasiosi. E' il caso della cosiddetta "giustizia predittiva", ossia della possibile elaborazione digitale mediante algoritmi di immense quantità di dati, per garantire alle parti o al giudice previsioni attendibili (quantificate sovente in termini percentuali) sul futuro. Si va, in pratica, dalla previsione delle decisioni giudiziarie su casi simili, utili alle difese per pronosticare il possibile esito di un'istanza o di un procedimento giudiziario ed articolare di conseguenza le proprie strategie[11], sino alla prognosi delle possibilità che l'indagato commetta reati o fugga o che il condannato si renda recidivo, utile al giudice, ad esempio, per decidere su una misura cautelare, sull'accesso al *probation* e persino sull'entità della pena irrogabile in concreto in caso di condanna. Rispetto a simili strumenti si segnalano i vantaggi in termini di certezza del diritto, innanzitutto, e persino di uguaglianza dei cittadini dinanzi alla legge[12], considerando che la prevedibilità delle decisioni su casi analoghi assicura la costruzione progressiva di orientamenti stabili e omogeneità negli esiti delle controversie o dei procedimenti. Anche dell'uso di strumenti predittivi nel campo esclusivamente penalistico, rispetto alle decisioni sull'imputato o indagato che tengano conto delle previsioni sui suoi comportamenti futuri, si può dir bene, nella misura in cui tendono a sostituire a valutazioni prognostiche del tutto soggettive (consistenti di regola in pronostici di pericolosità fatti in ragione della "fedina penale" del prevenuto e in base all'esperienza e alla sensibilità di

---

[10] Sulla riduzione del sovraffollamento carcerario come sfida da gestire con mezzi di sorveglianza elettronica sia della prospettiva di garantire il rispetto dei diritti umani, che in quella di assicurare l'efficiente gestione delle istituzioni penitenziarie, si concentra anche il preambolo della Raccomandazione CM/Rec(2014)4 del Comitato dei Ministri sulla sorveglianza elettronica.

[11] Cfr. L. Viola, voce *Giustizia predittiva*, in *Enciclopedia Treccani*, *Diritto-on-line*, p. 2.

[12] L. Viola, voce *Giustizia predittiva*, cit., *passim*; v. anche C. Castelli, D. Piana, *Giustizia predittiva. La qualità della giustizia in due tempi*, in www.questionegiustizia.it, 15 maggio 2018, p. 8.

chi giudica), verifiche basate sull'inattaccabilità equanime di un algoritmo, che può tenere conto di un'immensa quantità di dati e razionalizzarli in una previsione solida[13] e semplice, rappresentata in termini percentuali o su una scala di immediata comprensione (ad esempio, sulla pericolosità dell'imputato, da *low* a *high*)[14].

3. I RISCHI

Perché, dunque, non dovremmo aderire entusiasticamente all'uso ampio dello strumentario messoci a disposizione dalla moderna tecnologia per gestire il procedimento penale, a tutti i livelli e ovunque possibile? La realtà è che, naturalmente, le soluzioni inedite che lo sviluppo tecnologico propone al sistema - e che in esso stanno già trovando ampi spazi di attuazione o almeno di sperimentazione - non solo offrono nuove opportunità, ma pongono anche nuove sfide. Si tratta di problemi di compatibilità dei nuovi strumenti con l'impianto e la fisionomia "tradizionali" delle garanzie, di fatto riconducibili ad alcuni denominatori comuni: la protezione dei diritti fondamentali dei singoli; la fisionomia dei canoni fondanti di un processo equo (nella terminologia sovranazionale) e giusto (nella terminologia italiana); persino la potenziale metamorfosi di alcuni tratti qualificanti della giustizia penale come ingranaggio basilare della *res publica*.

Il primo elemento – di fatto comune a molte delle possibili strategie di impiego della tecnologia nel processo – è quello dell'esigenza di avvalersi in sede penale (e dunque in un delicatissimo settore al servizio della collettività) di prodotti di aziende private, come i programmi informatici, i *risk assessment tools* basati sugli algoritmi, gli strumenti di captazione o di sorveglianza elettronica, per la gestione dei quali è spesso necessario avvalersi dei servizi dei privati che producono la tecnologia acquistata

---

[13] Significativa l'osservazione che segue: «*Imagine a situation where the officer has the benefit of a hundred thousand, and more, real previous experiences of custody decisions? (...) no one person can have that number of experiences, but a machine can*» (University of Cambridge, *Helping police make custody decisions using artificial intelligence*, 26 febbraio 2018, in www.cam.ac.uk).

[14] M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., p. 3.

e che soli dispongono del *know how* per garantirne il funzionamento e la supervisione. Si tratta di una situazione per molti versi inedita, che fa virare sensibilmente il sistema penale (anche dove per tradizione ne è alieno, come nel caso italiano) verso una progressiva privatizzazione di aree rilevanti dell'amministrazione giudiziaria. Il fenomeno ha ricadute delicatissime su molti piani e produce conseguenze pratiche, che finiscono poi con l'impattare in maniera marcata sul sistema giuridico e sulla tutela dei diritti coinvolti in vari modi. Emblematico il caso del braccialetto elettronico in Italia, per il quale si è posto il problema di garantire gli arresti domiciliari rafforzati dalla sorveglianza elettronica, in alternativa alla custodia carceraria, laddove non fossero disponibili braccialetti a sufficienza. Poiché la legge prevede che il braccialetto elettronico venga applicato quando il giudice abbia verificato la disponibilità del dispositivo presso la polizia giudiziaria (art. 275 *bis* c.p.p.), ci si è chiesti cosa si dovesse fare nel caso in cui tale disponibilità non ci fosse. Si prospettavano per questa evenienza varie alternative, ossia: che il giudice dovesse ripiegare sugli arresti domiciliari in forma semplice (riespandendo l'area della libertà personale in presenza dell'impossibilità di monitoraggio elettronico); che si dovesse applicare a quel punto la custodia in carcere (passando a un livello più alto della compressione della libertà, benché ritenuto non necessario in prima battuta); o che si potessero formare liste d'attesa di soggetti che, trattenuti in carcere nelle more, dovessero attendere che i dispositivi si rendessero disponibili (affidando alle aziende addette all'installazione la gestione delle liste)[15]. Interpellate sul punto, le Sezioni Unite hanno affermato che in simili evenienze il giudice debba reiterare il vaglio di adeguatezza della misura cautelare e scegliere di nuovo tra arresti domiciliari e custodia carceraria, dovendosi respingere qualsivoglia automatismo nell'applicazione delle restrizioni della libertà personale[16]. Ma in seno al contrasto giurisprudenziale su

[15] Per una compiuta ricostruzione del quadro, v. E. Valentini, *Arresti domiciliari e indisponibilità del braccialetto elettronico: è il momento delle Sezioni Unite*, in *www.penalecontemporaneo.it*, 27 aprile 2016, p. 6 ss.

[16] Cass., sez. un., 28 aprile 2016, Lovisi, in CED 266651. Per un commento, v. I. Guerini, *Più braccialetti (ma non necessariamente meno carcere): le Sezioni Unite e la portata applicativa degli arresti domiciliari con la procedura di controllo del braccialetto elettronico*, in www.penalcontemporaneo.it, 24 giugno 2016.

questo tema sono emerse sottolineature interessanti, ad esempio laddove la Suprema Corte ha sottolineato come non debba ritenersi obbligo dello Stato acquistare abbastanza braccialetti elettronici da coprire le esigenze di tutti coloro che vi avrebbero diritto, essendo limitate le risorse dello Stato e dunque le prestazioni che i cittadini possono aspettarsi di ricevere[17]. La privatizzazione della tecnologia di impiego giudiziario, insomma, a tacer d'altro, spinge a considerare gli strumenti di limitazione della libertà personale che presidiano la riduzione della compressione indispensabile di libertà come un "servizio" monetizzabile, connotato da costi inesigibili in termini generalizzati e che finiscono quindi per essere un privilegio di pochi (accidentalmente) fortunati[18].

La dipendenza del sistema pubblico dall'impresa privata, poi, può avere ricadute anche più sottili e insidiose. E' il caso degli algoritmi predittivi, utilizzabili dai giudici per prendere decisioni sul rischio di recidiva o di fuga e dunque sia a fini cautelari, sia per l'accesso al misure di *diversion* a vario livello, e persino sulla commisurazione della pena. In tal caso, infatti, l'esperienza statunitense ha mostrato come si ponga seriamente il problema della compatibilità tra il diritto di difesa e la protezione della proprietà intellettuale sul programma usato, che fondamentalmente comporta la segretezza del funzionamento dell'algoritmo che il giudice ha usato per la decisione[19]. In altri termini, c'è il rischio che il giudice possa

---

[17] Cass., 17 settembre 2014, n. 520, in *De Jure*.

[18] V. più ampiamente *infra*, D. Negri, cit. Si tratta di un problema cardine del tema in esame, se si considera che il panorama delle giurisdizioni in cui la sorveglianza elettronica è utilizzata mostra soluzioni variegate: il dato è esplicitamente ammesso dalla Raccomandazione Rec(2014)4 del Comitato dei ministri del Consiglio d'Europa sulla sorveglianza elettronica, che nel secondo paragrafo segnala che in alcuni paesi i costi dello strumento installato sul sospettato o condannato sono interamente a carico dello Stato, mentre altrove all'interessato si richiede di versare un contributo; tant'è che al § III, 11, si premura di specificare che in tal caso l'ammontare del contributo deve essere proporzionato alle condizioni finanziarie dell'interessato e regolato dalla legge. In tema, sui rischi di discriminazione a danno di chi versi in condizioni economiche disagiate, v. anche M. Black, R.G. Smith, *Electronic Monitoring in the Criminal Justice System*, in *Australian Institute of Criminology* <www.aic.gov>, Au, Maggio 2003, May 2003, p. 5.

[19] Si tratta di un problema, a rigore, anche più ampio: esso si pone negli stessi termini per ogni prova digitale, giacché è impossibile «falsificare il dato prodotto da un algoritmo se non è possibile accedere al codice sorgente che

decidere della libertà dell'imputato o della sanzione penale applicabile al condannato in base ad elementi che la difesa non è stata in grado di vagliare e contestare, non avendo accesso all'algoritmo che li ha forniti al giudice. Il problema, oggetto di acceso dibattito negli U.S.A., è stato affrontato a livello giurisprudenziale con una nota e controversa decisione, che ha ammesso che l'uso degli algoritmi sia consentito nel *sentencing*, purché non in via esclusiva, risultando anzi utile ad assicurare l'approdo a una decisione individualizzata, bastando ad assicurare il diritto di difesa che questa possa confutarne l'attendibilità facendo ricorso al manuale d'uso dello strumento[20]. Una soluzione il cui impianto logico e culturale non persuade: innanzitutto, il fatto che un'informazione non sia usata in modo esclusivo non toglie che abbia rilevanza nel giudizio (in modo peraltro imperscrutabile, se si tiene conto del peso psicologico che può esercitare sul giudicante il risultato di un algoritmo che non dà conto dei dati, ma li ricostruisce per vie misteriose in un "pacchetto decisorio" preconfezionato con una soluzione data); inoltre, il diritto di difesa nel suo significato minimale impone che possa essere oggetto di verifica (e sia quindi comprensibile e pienamente accessibile) qualunque contributo informativo suscettibile di influire sulla decisione, suggerendo valutazioni critiche degli elementi a disposizione che ne presuppongono la totale trasparenza.

Infine, si deve tenere conto dei rischi immanenti ad ogni caso in cui si debba affidare a privati la gestione di uno strumento tecnologicamente

---

governa l'algoritmo stesso», per cui quando la conoscenza immessa nel processo ha simile fonte, la segretezza del software (a tutela della proprietà intellettuale) preclude di per sé la verifica di attendibilità dei risultati probatori che la difesa dovrebbe sempre essere in condizione di fare (cfr. S. Quattrocolo, *Equità del processo penale*, cit., p.12).

[20] State vs. Loomis, 881 NW 2d 749 (Wis 2016), secondo cui, appunto, «*a COMPAS risk assessment is only one of many factors that may be considered and weighed at sentencing*» e «*a COMPAS risk assessment at sentencing along with other supporting factors is helpful in providing the sentencing court with as much information as possible in order to arrive at an individualized sentence*». La stessa decisione, peraltro, articola una serie di avvertimenti sull'utilizzo dello strumento, di fatto consigliando cautela nell'uso di simili algoritmi predittivi. Per un'analisi della vicenda, cfr. M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., p. 6 ss.; S. Quattrocolo, *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs. rischi e paure della giustizia digitale predittiva*, in *Cass. pen.*, 4, p. 1751 ss.

avanzato in sede penale, anche per la tendenza naturalmente espansiva di questi mezzi, capaci di proiettare il proprio impatto oltre i confini dell'uso cui sono destinati nel processo. E' il problema che si pone per la gestione dei dati personali che possono essere raccolti tramite prove digitali o strumenti di sorveglianza elettronica: si pensi all'immane quantità dei dati che si possono captare con i virus informatici o con la sorveglianza mediante GPS, e all'esigenza di porre regole e presidi sicuri per evitarne impieghi abusivi, stoccaggio e commercializzazione o diffusione incontrollati[21].

Altra categoria di problemi nuovi indotti dall'uso delle tecnologie avanzate in sede penale è quella dell'impatto sulle tradizionali aree di libertà garantite ai singoli, rispetto alle quali siamo avvezzi a una tipologia di aggressioni e limitazioni che poco ha oramai a che vedere con quella (spesso immateriale e quindi non avvertibile) collegata a mezzi tecnologicamente sofisticati. Per avvedersene, basta considerare le numerose implicazioni della sorveglianza elettronica mediante geolocalizzazione. Utilizzata in molti sistemi a vari fini, ha fatto ingresso silenziosamente anche nel sistema italiano, nel quale è impiegata sotto forma di pedinamento elettronico o come supporto indispensabile all'esecuzione di misure cautelari di nuovo conio previste a protezione della vittima e corrispondenti ai *restraining orders* anglosassoni, ossia l'allontanamento dalla casa familiare (art. 282 *bis* comma 6 c.p.p.) e il divieto di avvicinarsi alla persona offesa (art. 282 *ter* comma 1 c.p.p.)[22]. Si tratta di misure il cui contenuto consiste non nell'obbligo di restare in un determinato luogo o entro un perimetro predefinito, ma, al contrario, nel non rientrarvi, o addirittura nel non accostarsi a una persona (la vittima), a un gruppo di persone (familiari e partner della vittima) o a determinati posti (quelli frequentati dalla vittima o da persone a lei vicine), interessando dunque una pluralità di luoghi a spettro variabile. Il controllo sul rispetto delle prescrizioni imposte in

[21] La Raccomandazione del Comitato dei Ministri CM/Rec(2014)4 sulla sorveglianza elettronica puntualizza, infatti, che la raccolta di dati attraverso il monitoraggio vada regolata dalla legge, garantendo trasparenza e protezione da utilizzi arbitrari (§ VI).

[22] Gli aggiornamenti delle due previsioni proprio per consentire l'uso delle «particolari modalità di controllo previste dall'articolo 275 *bis*» si devono rispettivamente al d.l. 14 agosto 2013 n. 93, conv. L. 15 ottobre 2013 n. 119 e, assai di recente, alla l. 19 luglio 2019 n. 69.

questi casi non può che essere fatto con uno strumento di sorveglianza "globale", che monitori in tempo reale ogni spostamento della persona soggetta al provvedimento restrittivo, controllandola per forza di cose ben oltre il necessario ed apprendendo informazioni innumerevoli sulle sue abitudini, spostamenti e frequentazioni, coinvolgendo persino la persona offesa, che viene controllata di riflesso. Si tratta di una prospettiva che pone seri problemi in punto di principio di proporzionalità, ad esempio, giacché la limitazione di libertà che consegue all'uso dello strumento di controllo è maggiore di quella consentita di per sé dalla misura adottata e calibrata sull'effettiva necessità. Senza dire delle incognite che si addensano sullo stesso principio di legalità, che dovrebbe presiedere all'individuazione del quando, se e come limitare la libertà personale dei singoli e che è minacciato da strumenti la cui misura di invasività rischia di essere di fatto affidata a un'evoluzione tecnologica cui il sistema giuridico tende ad adeguarsi mediante provvedimenti non legislativi (più agili e adatti ad assecondare il progresso rapidissimo della scienza) e che è di fatto gestita da privati. Non è un caso, infatti, se la Raccomandazione del Comitato dei Ministri CM/Rec(2014)4 sulla sorveglianza elettronica si preoccupa di sancire garanzie minime proprio su questi aspetti, ad esempio stabilendo l'esigenza: che sia una legge a prevedere casi, modi e durata della sorveglianza elettronica (§ III, 1), che essa debba rispondere al principio di proporzionalità (§ III, 4), che non possa essere utilizzata oltre i limiti stabiliti dalla decisione che la prescrive (§ III, 5) e che per il coinvolgimento della vittima occorra il suo consenso (§ IV, 18).

Del resto, proprio gli strumenti di monitoraggio a distanza mostrano come il ricorso alle nuove tecnologie possa essere un'opportunità, ma anche fonte di nuovi rischi allo stesso tempo, essendo spesso gli strumenti impiegati suscettibili di un uso "bifronte" e portatori di profonde ambiguità. La sorveglianza elettronica può essere uno strumento di decarcerizzazione, ad esempio, garantendo fra l'altro la possibilità per il prevenuto o per il condannato di non entrare in carcere e di non subire quel distacco dal contesto familiare e sociale che è fonte di straniamento e costituisce poi il principale ostacolo alla risocializzazione necessaria a contenere il rischio di recidiva. Tuttavia, il controllo a distanza non basta a questi fini e potrebbe costituire un facile alibi per non approntare i programmi e i servizi di supporto sociale che sono comunque indispensabili per

garantire una risocializzazione effettiva ed evitare l'emarginazione di imputati e condannati; inoltre, il controllo elettronico porta con sé un carico psicologico autonomo, del tutto peculiare, con effetti potenzialmente negativi (se non gestiti adeguatamente) sia sul protagonista che sulla comunità di riferimento[23]. Di nuovo, su questo è significativo che la Raccomandazione CM/Rec(2014)4 sottolinei più volte come l'applicazione di misure di sorveglianza elettronica andrebbe combinata con interventi professionali e di sostegno mirati alla reintegrazione sociale del prevenuto e che si deve evitare che esse sfocino in forme di isolamento o esclusione (§ III, 8 e § IV 19 e 21).

Va aggiunto a queste considerazioni non solo che l'uso della tecnologia nel processo si pone talora in tensione con i fondamentali diritti dei singoli e mette alla prova le garanzie che li circondano, ma anche che la società a tecnologia avanzata introduce nel sistema concetti nuovi, che si collocano lungo i confini semantici degli istituti "tradizionali" e ne forzano il senso, sfidando l'interprete a stabilire dove collocarli. A titolo di esempio, si guardi al concetto di "identità digitale"[24] (il *nickname* o l'*avatar* di chi svolge attività in rete, talora vivendo in essa vere e proprie vite parallele) dell'imputato e al problema se sia coperto dal diritto al silenzio come ogni altra informazione che questi possa fornire al procedimento o se rientri nella sfera delle «generalità» e di «quant'altro può valere a identificarlo» che vi è sottratto *ex* art. 66 del codice di rito italiano. Ove si ritenga che le coordinate identificative della "persona digitale" siano ascrivibili a quest'area concettuale, l'imputato non potrebbe avvalersi dello *ius tacendi* rispetto ad esse ed avrebbe l'obbligo di rivelarle agli inquirenti[25]. Si tratta di interpretazione plausibile, anche se non persuade del tutto che

---

[23] Interessante, su questo punto, la rapida panoramica di opinioni sull'esperienza australiana, in M. Herbert, *Fears Australia being turned "into a prison" after surge in electronic monitoring of offenders*, in *Australian news*-in www.theguardian.com, 31 agosto 2019. V. altresì le preoccupazioni già segnalate in M. Black, R.G. Smith, *Electronic Monitoring*, cit., p. 4 s.

[24] Cfr. G. Alpa, *Il diritto di privati. Profili attuali del diritto delle persone*, R.E. Kostoris (a cura di), *Percorsi giuridici della postmodernità*, Il Mulino, 2016, p. 164 ss., che la considera oggetto di un autonomo diritto.

[25] In tal senso, S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 34 s., ove si precisa che invece le *passwords* e le chiavi elettroniche rientrano comunque nell'area del diritto al

si possano desumere da una lettura estensiva della norma – certamente pensata per l'identificazione di una persona fisica e non del suo alter ego digitale – erosioni di un diritto fondamentale come il diritto al silenzio, le cui limitazioni dovrebbero essere (in quanto eccezionali) previste con precisione e inestensibili oltre i confini delineati esplicitamente dalla legge[26]. Proprio per questo, però, il tema evidenzia come la tecnologia imponga la rilettura delle norme, la ridefinizione delle categorie fondanti, insomma uno sforzo esegetico chiamato a colmare le lacune di un tessuto normativo destinato a divenire obsoleto se il legislatore non provvede ad aggiornarlo con uno sforzo consapevole e un'adeguata riflessione.

Infine, la tecnologia impiegata nel processo è potenzialmente capace di metterne in discussione addirittura i pilastri, sistematici e culturali, prima ancora che giuridici. E' il caso dell'impiego degli algoritmi nell'adozione di decisioni che presuppongono il vaglio del rischio individuale (in genere, di fuga o di recidiva), già più volte rammentati. L'ingresso per questa via dell'uso dell'intelligenza artificiale nel sistema penale è probabilmente quello che più si approssima alla fantascienza, se non fosse che si tratta ormai di una realtà, che in molti paesi ha avuto un notevole sviluppo nell'ultimo decennio. Le incognite di un simile utilizzo, che ai più appare ragionevolmente inevitabile, sono numerose ed investono molti delicati profili di un punto chiave del sistema, come l'adozione delle decisioni giudiziali, imponendo una riflessione immediata, preziosa per sistemi come quello italiano, in cui esperienze di questo genere non sono ancora attuali, ma futuribili. Nel dibattito di matrice anglo-americana su questi temi[27], ad esempio, emerge la forte convinzione che l'uso degli algoritmi valga a rendere più oggettive e rapide le decisioni: un giudice che potrebbe fare affidamento di regola solo sulla propria esperienza e su pochi dati significativi relativi a un accusato, come i precedenti penali, potrebbe ricevere un utile aiuto dagli algoritmi predittivi, idonei a fornirgli

silenzio in quanto finalizzate non a identificare un soggetto, quanto a proteggere le informazioni che immette nel sistema.

[26] Del resto, si può immaginare che in molti casi di reati commessi tramite mezzi informatici, esigere che l'imputato riveli la sua identità digitale equivale di fatto a pretendere che confessi.

[27] Per i riferimenti fondamentali, si rinvia a M. Gialuz, *Quando la giustizia penale*, cit., *passim*.

una valutazione del pericolo di fuga o di commissione di nuovi reati in una forma di immediata percezione (su un'ipotetica scala di rischio o con un numero percentuale) già pronta all'uso. Giacché l'algoritmo lavora sulla base oggettiva di una formula matematica che elabora una mole immensa di dati immessi nel programma e relativi a molteplici fattori reputati rilevanti ai fini del calcolo dei rischi di fuga o di recidiva dei singoli (età, lavoro, stato di famiglia, precedenti e molti altri), a prima vista snellisce il lavoro del giudice. Gli offre infatti un "pacchetto finale", in cui converge una mole di informazioni che da solo non potrebbe mai conoscere, ed opera nel modo tipico delle intelligenze artificiali, ossia "neutrale" e dunque equo e obiettivo. Inoltre, sembra oramai consolidata a vari livelli la consapevolezza che la valutazione dell'algoritmo non potrebbe mai sostituirsi alla decisione "umana", nella quale il giudice resta sovrano; un canone di fondo che si traduce, negli U.S.A., nell'affermazione che vuole che gli algoritmi predittivi possano essere impiegati solo a conforto di altri elementi di prova capaci di sostenere la decisione anche da soli; e, in Europa, nel principio che vieta di prendere decisioni a carico di singoli esclusivamente in base a programmi di profilazione dei dati[28]. Questo panorama, tuttavia, lascia più d'una perplessità.

Dell'oggettività e accuratezza degli algoritmi, innanzitutto, c'è ragione di dubitare, se è vero che alcuni sono stati criticati proprio per

[28] Il punto è chiarito all'art. 11 della Direttiva 2016/680/UE (per un'analisi critica, v. M. Gialuz, *Quando la giustizia penale*, cit., p. 16 s.). Sembra andare in questo senso anche il principio del "controllo da parte dell'utente", affermato nella *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia*, adottata dalla Commissione per l'efficienza della giustizia del Consiglio d'Europa il 4 dicembre 2018 (CEPEJ). Il principio ha un'applicazione ampia e qualche margine di ambiguità ma, per quanto riguarda il giudice, sembra implicare che la decisione non possa essere legata in modo vincolante a trattamenti automatizzati di dati, che il giudice deve poter gestire in piena consapevolezza ed autonomia; per un commento a prima lettura, v. S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali ed informatiche*, in www.lalegislazionepenale.it, 18 dicembre 2018, spec. p. 9 s. Del resto, si deve evitare il rischio che l'impiego degli algoritmi decisori in sede penale dia accesso in sede penale ai programmi di "profilazione", atti a convertire surrettiziamente il processo in rito penale del tipo d'autore; si tratta di un pericolo che la dottrina più avvertita segnala (v. M. Gialuz, *Quando la giustizia penale*, cit., p. 421).

la loro attitudine a fornire responsi discriminatori (utilizzando dati sulla razza, ad esempio) e perché la loro scarsa trasparenza di funzionamento comporta l'opacità della selezione dei dati rilevanti e del "peso" loro assegnato all'interno del computo finale[29]. Che agevolino la decisione del giudice e la rendano più rapida non si dubita, ma il prezzo potrebbe essere la sudditanza di fatto del giudizio umano a quello della macchina: considerando la tendenza umana a fidarsi degli esiti di un processo computerizzato[30], c'è il serio rischio che il giudicante finisca con il delegare all'algoritmo il peso della decisione; non conforta che debbano esservi altri elementi a sostegno di questa, in fin dei conti, giacché un giudice può sempre trovare in atti la giustificazione ragionevole della sua decisione, specie per valutazioni predittive che già di regola poggiano su basi non solide, anche quando ha maturato il proprio convincimento in pochi secondi sul responso dell'intelligenza artificiale[31]. L'affidabilità di questa e la sua neutralità, poi, non persuadono: la componente di freddezza razionale che sembra assicurare credibilità alla decisione, non la rende in realtà migliore; la decisione umana porta con sé l'idea della comprensione, del vaglio ragionevole (fatto anche di una componente di intelligenza emotiva) delle caratteristiche dell'individuo che è comparso innanzi al giudicante, nonché della responsabilità (il cui peso è avvertito solo da un essere umano e che è elemento rassicurante della prudenza nel decidere e giustificativo della affidabilità dell'esito anche di fronte alla collettività). Tutte queste componenti rischiano di annacquarsi (o, peggio, perdersi), a fronte di un utilizzo meno che prudente di strumenti di intelligenza artificiale nel processo decisionale.

---

[29] Tra gli altri, J. Dressel, H. Farid, *The accuracy, fairness, and limits od predicting recidivism*, in www.advances.sciencemag.org, 30 marzo 2018.

[30] Si tratta di fenomeno studiato in altri campi e definito *automation bias*, «*which occurs when a human decision maker disregards or does not search for contradicory information in light of a computer-generated solution which is accepted as correct. Operators are likely to turn over decision processes to automation as much as possible due to a cogntivie conservation phenomenon, and teams of people, as well as individuals, are susceptible ti automation bias*» (M.L. Cummings, *Automation bias in Intelligent Time Critical Decision Support Systems*, in htpps://arc.aiaa.org, 19 giugno 2012, p. 2).

[31] Il "pregio" dell'algoritmo sta proprio nel fatto che non fornisce i dati raccolti ed elaborati, ma il solo risultato finale del computo.

Che questi, comunque, premano alle porte dei sistemi che ancora non ne fanno uso a livello processuale, è evidente a partire dalla situazione italiana, in cui la giustizia predittiva sembra avere fatto capolino solo nell'ambito dell'attività di controllo del territorio ad opera delle forze di polizia[32], ma - per ora - non a livello processuale. Tuttavia, si sta già cominciando a ragionare dei possibili spazi applicativi che potrebbe trovare nel procedimento, a partire dal vaglio del pericolo di fuga e del rischio di recidiva in sede di applicazione delle misure cautelari (art. 274 c.p.p.), sino ai canoni di commisurazione della pena *ex* art. 133 c.p.: entrambe valutazioni che potrebbero in astratto giovarsi dell'applicazione degli algoritmi predittivi, se non fossero basate a livello normativo su indicatori che paiono descritti volutamente in termini oggettivi[33], oltre che rigorosamente individualizzanti. Anzi, l'ambito a ben guardare potrebbe anche essere più ampio, se si considera che l'art. 133 c.p. fa da punto di riferimento anche per il vaglio sull'accesso alla sospensione del processo con messa alla prova, misura di *probation* processuale che – in modo non dissimile dagli istituti affini di stampo anglosassone – si fonda in maniera significativa sulla concedibilità a soggetti che non abbiano elevata pericolosità. Naturalmente, il sistema italiano reca ancora un freno rilevante all'impiego di simili mezzi nell'art. 220 c.p.p., che vieta la prova scientifica sul carattere e sulla personalità (nonché sulla tendenza a delinquere) dell'imputato, così (si direbbe) vietando anche quella forma di "appalto tecnologico" del medesimo giudizio a base scientifico-matematica che sarebbe legato all'uso degli algoritmi. Tuttavia, vi è chi osserva che gli algoritmi predittivi non comportano di per sé un accertamento personologico, ma il mero calcolo dei rischi rispetto a probabilità di tenuta di specifiche condotte future, sicché potrebbero teoricamente sfuggire al rigore del divieto posto dal codice[34]. Senza considerare che vi sono spazi significativi del sistema, come quello minorile, ad esempio, in cui quel

---

[32] Si allude al noto *Key crime*, adottato dalla Questura di Milano, e all' *X-Law*, software elaborato dalla Questura di Napoli e adottato in molte altre sedi.

[33] M. Gialuz, *Quando la giustizia penale*, cit., p. 19.

[34] Così M. Gialuz, *Quando la giustizia penale*, cit., p. 20, dove si osserva anche che l'alternativa, in ordine sia alle limitazioni di libertà personale, che alla quantificazione della pena, è pur sempre affidarsi all'intuito (o all'arbitrio) del giudicante.

divieto non opera e anzi in ordine alle valutazioni personologiche impera (per espressa autorizzazione legislativa, *ex* art. 9 comma 2 d.P.R. n. 448 del 1988) un'insidiosa libertà di forme, nella quale qualunque strumento potrebbe in futuro innestarsi[35].

4. Conclusioni

Il panorama descritto, sia pure assai parziale, vale solo a rappresentare quanto le nuove tecnologie possano avere sul sistema processualpenalistico un impatto non solo rilevante, ma addirittura dirompente. Atte a scardinarne persino le categorie fondanti ed entrare in tensione in modo del tutto inedito con i diritti fondamentali dei singoli, esse sono tuttavia una componente imprescindibile del nostro mondo e sarebbe improvvido rifiutare di considerarne le implicazioni anche in questo settore, nel quale sono già penetrati (in molti sistemi) o alle cui porte premono energicamente.

Si può e si deve, quindi, ragionare sui possibili spazi applicativi dei prodotti più avanzati dell'evoluzione tecnologica nel processo, per non lasciarsi sfuggire l'opportunità di garantire ai sistemi maggiore efficacia ed efficienza, ma anche per valutarne i rischi, nell'ottica di una tempestiva predisposizione delle necessarie garanzie. In questa prospettiva, sarà indispensabile rileggere le garanzie esistenti in chiave innovativa, ma anche congegnarne di nuove, per strutturare la tutela dei diritti umani e i principi cardine del giusto processo in modo adeguato ad affrontare il modificarsi della realtà processuale in sintonia con l'evoluzione del sistema verso una società tecnologicamente nuova.

E' questo lo scopo dei contributi che seguono: offrire, senza pretese di completezza, una panoramica dei problemi, delle opportunità, degli

---

[35] L'impiego massiccio di questo strumentario in ambito minorile, del resto, sembra esserne una costante nei contesti in cui è già consolidato: si veda, a titolo di esempio, l'esperienza statunitense, in cui il fenomeno pare massicciamente in espansione: M. Gialuz, *Quando la giustizia penale*, cit., p. 4. Non è in caso, dunque, se è proprio in tale ambito che si comincino a segnalare negli U.S.A. decisioni che reclamano solidi standard di serietà scientifica per gli strumenti da impiegare nel processo (v. S. Quattrocolo, *Intelligenza artificiale e giustizia*, cit., p. 11).

spunti di analisi critica, che l'impatto delle nuove tecnologie nel processo penale solleva e sollecita, in modo da contribuire a una riflessione comune che appare necessaria. Se il cambiamento è inevitabile, è indispensabile non farsi cogliere impreparati.

Bibliografia

ALPA, Guido. *Il diritto di privati. Profili attuali del diritto delle persone*, R.E. Lostoris (a cura di), *Percorsi giuridici della postmodernità*, Il Mulino, 2016, p. 164 s

BLACK, Matt; SMITH, Russell G. *Electronic Monitoring in the Criminal Justice System*, in *Australian Institute of Criminology* < in www.aic.gov.>, May 2003, p. 5.

BRONZO, Pasquale. *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in G. Giostra, R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni*, Giappichelli, 2018, p. 235 s.

BUZZELLI, Silvia. *Le modifiche alla disciplina della partecipazione a distanza*, in L. Giuliani, R. Orlandi (a cura di), *Indagini preliminari e giudizio di primo grado*, Giappichelli, 2018, p. 73 s.

CAMON, Alberto. *Cavalli di Troia in Cassazione*, *Arch. nuova proc. pen*., 2017, p. 91.

CAPRIOLI, Francesco. *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista Brasileira de Direito Processual Penal*, 2017, n. 3, p. 483 s.

CASTELLI, Claudio; PIANA, Daniela. *Giustizia predittiva. La qualità della giustizia in due tempi*, in www.questionegiustizia.it, 15 maggio 2018, p. 8.

CESARIS, Laura. *Dal* panopticon *alla sorveglianza elettronica*, in M.Bargis (a cura di*), Il decreto "antiscarcerazioni"*, Giappichelli, 2001, p. 51 s.

CUMMINGS, Mary L. *Automation bias in Intelligent Time Critical Decision Support Systems*, in <htpps://arc.aiaa.org>, 19 giugno 2012, p. 2

DANIELE, Marcello. *La sagomatura dell'esame a distanza nel perimetro del contraddittorio*, in D. Negri, R. Orlandi (a cura di), *Le erosioni silenziose al contraddittorio,* Giappichelli, 2017, p. 133.

DANIELE, Marcello. *La formazione digitale delle prove dichiarative*, Giappichelli, 2012, p. 7 s.

DI PAOLO, Gabriella. *"Tecnologie del controllo" e prova penale*, Cedam, 2008, p. 251 s.

DRESSEL, Julie; FARID, Hany. *The accuracy, fairness, and limits od predicting recidivism*, in www.advances.sciencemag.org, 30 marzo 2018.

GIALUZ, Mitja. *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *www.dirittopenalecontemporaneo.it*, 29 maggio 2019, p.3.

GUERINI, Irene. *Più braccialetti (ma non necessariamente meno carcere): le Sezioni Unite e la portata applicativa degli arresti domiciliari con la procedura di controllo del braccialetto elettronico*, in www.penalcontemporaneo.it, 24 giugno 2016.

HERBERT, Miles. *Fears Australia being turned "into a prison" after surge in electronic monitoring of offenders*, in *Australian news*-in www.theguardian.com, 31 agosto 2019.

NEGRI, Daniele. *Nuove tecnologie e compressione della libertà personale: la sorveglianza con dispositivi elettronici dell'imputato sottoposto a misure cautelari*.

PITTIRUTI, Marco. *Digital evidence e procedimento penale*, Giappichelli, 2017, p. 8.

QUATTROCOLO, Serena. *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uom*o, in *Revista Italo-Espanola de derecho procesal*, 2019, p. 3.

QUATTROCOLO, Serena. *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs. rischi e paure della giustizia digitale predittiva*, in *Cass. pen*., 2019, 4, p. 1751 ss.

QUATTROCOLO, Serena. *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali ed informatiche*, in www.lalegislazionepenale.it, 18 dicembre 2018, spec. p. 9 s.

RIVELLO, Pier Paolo. *Le intercettazioni mediante captatore informatico*, in O. Mazza (a cura di), *Le nuove intercettazioni*, Giappichelli, 2018, p. 102 s.

SERRANI, Alessandro. *Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie*, in *Arch. pen.* (web), 2013, n. 3.

SIGNORATO, Silvia. *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 34 s.

SIGNORATO, Silvia. *Modalità procedimentali dell'intercettazione tramite captatore informatico*, in G. Giostra, R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni*, Giappichelli, 2018, p. 263 s.

TESTAGUZZA, Alessandra. Digital forensics. *Informatica giuridica e processo penale*, Cedam, 2015, p. 2 s.

VIOLA, Luigi. voce *Giustizia predittiva*, in *Enciclopedia Treccani*, *Diritto-on-line*, p. 2.

Informações adicionais e declarações do autor
(*integridade científica*)

Declaração de conflito de interesses (conflict of interest declaration): a autora confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste editorial.

Declaração de autoria (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste editorial estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

Declaração de ineditismo e originalidade (declaration of originality): A autora assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

COMO CITAR ESTE EDITORIAL:

CESARI, Claudia. Editoriale: L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 4, n. 3, p. 1167-1188, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.292

Using New Means of Technology during the Penal Proceedings in Romania

El uso de nuevos medios tecnológicos en el procedimiento penal en Rumanía

O uso de novos meios de tecnologia no processo penal da Romênia

Delia Magherescu[1]
Gorj Bar Association – Romania
delia_magherescu@yahoo.com
http://orcid.org/0000-0003-0939-1549

Abstract: The new legal framework created since 2014 while the new Code of penal procedure entered into force in Romania has opened a different way of approaching the justice in criminal matters. In such a legal context the judicial bodies are more accustomed with the idea of using the new means of technology in such a way not to infringe the parties' procedural rights during the penal trial knowing the fact that using illegal protocols signed by the prosecutor offices with the Romanian Intelligence Service was prohibited by the Constitutional Court of Romania. In the current paper, a qualitative research has been carried out on both legislative and jurisprudence items regarding the new means of technologies currently used in the penal justice. The main purpose of the paper is to analyze the effect of the new means of technology including the use of digital evidence which occur in the penal trial in Romania as well as to discuss the legal consequences they produce in practice. Some practical points of view have been highlighted taking into account the new means of technologies' efficiency. Moreover, in order to improve the penal procedure into force certain proposals of *de lege ferenda* have been provided.

Keywords: means of technology; digital evidence; procedural issues; respecting parties' rights; constitutional limitation.

[1] Doctor in Law since 2005 awarded at the State University of Moldova, Republic of Moldova.

Resumen: *El nuevo marco jurídico creado en Rumanía en 2014, con la aprobación de un nuevo Código de procedimiento penal, ha transformado la forma de aproximación a la justicia penal. En este contexto jurídico, los entes jurisdiccionales se han ido adaptando a usar nuevos medios tecnológicos en el marco de los procedimientos penales sin infringir los derechos procesales de las partes, tras la prohibición, por parte del Tribunal Constitucional, del empleo de protocolos ilegales firmados por las fiscalías con el Servicio de Inteligencia de Rumanía. En este trabajo se desarrolla una investigación cualitativa, que analiza materiales legislativos y jurisprudenciales, sobre los nuevos medios tecnológicos que se usan en la justicia penal. El objetivo principal del artículo es analizar los efectos de esos nuevos medios tecnológicos empleados en el procedimiento, incluidas las pruebas digitales, así como discutir las consecuencias jurídicas que producen en la práctica. En este sentido, se ponen de relieve algunos puntos de vista prácticos que destacan la eficiencia de los nuevos medios tecnológicos. Junto a ello, se hacen algunas propuestas de lege ferenda para mejorar el procedimiento penal en vigor.*

Palabras-clave: *medios tecnológicos; prueba digital; cuestiones procesales; garantía de los derechos de las partes; límites constitucionales.*

Resumo: *O novo quadro legal criado em 2014, quando da entrada em vigor do novo Código de Processo Penal na Romênia, deixou aberta uma nova forma de aproximação à justiça criminal. Nesse contexto legal, as autoridades judiciais estão mais habituadas a usar os novos meios tecnológicos de modo a não infringir os direitos processuais das partes durante o julgamento, sabendo que o uso de meios ou protocolos ilegais, assinados pela acusação em conjunto com o serviço de informação da Romênia, é proibido pelo Tribunal Constitucional da Romênia. No presente estudo, analisam-se alguns aspectos dos novos meios tecnológicos que são atualmente usados na justiça penal, tanto no plano legislativo como jurisprudencial. O propósito principal deste estudo é analisar o efeito dos novos meios tecnológicos, incluindo a prova digital, utilizados em julgamentos criminais na Romênia, bem como discutir as consequências legais da sua utilização. Alguns aspetos práticos foram sublinhados tendo em conta a eficiência desses novos meios tecnológicos. Apresentam-se ainda algumas propostas de lege ferenda de modo potenciar a realização do processo penal.*

Palavras-chave: *meios tecnológicos; prova digital; questões processuais; direitos processuais; limites constitucionais.*

Introduction

Romania has followed a well structured way determined by the judicial authorities' goals to achieve the European general legal framework of reorganizing the entire judicial system in criminal matters in accordance with the democratic values since January 1, 2007 while it joined the European Union as a Member State. Nevertheless, that way was not a smooth one due to the fact that Romania is coming after a long and difficult transition period from the totalitarian regime to democracy and the rule of law principles. In this both social and legal context, it is relevant for the judicial authorities the European programs of harmonizing the home legislation in criminal matters to the European acquis. These efforts have been also made previously more particularly during the ante-adhesion period, but the real reformation of the judicial system in criminal matters started since 2007. From this reason, I appreciate the "*judicial spring*" has begun in 2014 once the Law no. 135/2010 on the new Code of penal procedure entered into force.[2] Thus, the long time-period states a difficult itinerary but necessary in order for the Romanian authorities to reach the proposed scope.

The new Code of penal procedure has the main role of regulating new judicial institutions, one of them leads with the implementation of the new means of technology in the justice in criminal matters. As it will be highlighted in the current paper, the new means of technology used in the investigation of penal cases created the opportunity to achieve the most appropriate procedure of solving the penal cases, on the one hand. On the other hand, there were some special techniques of criminal investigation that produced an interference in the parties' fundamental rights exercised during the penal trial. They have been more reflected in the defendant's procedural rights during the criminal proceedings.

It is well known at the moment one of the objectives of the penal trial is that of *implementing the digital world* in the penal proceedings as a result of adapting the new legislation in the field of penal procedure law

[2] Law no. 135/2010 on the Code of penal procedure of Romania, published in the Romanian Official Journal no. 486 of 15 July 2010, entered into force on February 1, 2014.

to the contemporary social changes. For the Romanian judicial system in criminal matters it was very much a desideratum. Nevertheless, it is one of the legal ways of finding adequate solutions for the judicial and technical issues the judicial bodies are still confronted with.[3]

In the field of jurisprudence, the main objective is that of harmonizing the modern technical means of investigation in the penal cases with respecting the participants' fundamental rights during the penal proceedings. From this point of view, the doctrine has emphasized the idea of avoiding two issues both by the legislator and the judicial bodies called to apply the provisions of the Code of penal procedure in their activity of solving the penal cases.

Thus, on the one hand the formalism of pronouncing the judicial solutions which are impossible to apply in practice must be avoided.[4] On the other hand, the formalism of pronouncing practical and pragmatic solutions which do not assure respecting the fundamental parties' rights as well.[5]

In carrying out the current research paper, I analyzed the doctrinaire points of view as well as the jurisprudence references gathered from the law courts' decisions pronounced in penal cases. They allowed me to point out some pertinent statements on the most relevant aspects the means of technology occur in the penal trial in Romania.

1. Digital evidence: an overview

During the investigation phase of the penal trial, the investigation bodies' scope is that of gathering evidence in order to find the truth in the penal cases they were invested with. Actually, the scope of the investigation phase must be viewed in accordance with the scope of the entire penal trial due to the fact that the decision pronounced will reflect the truth if it is based on evidence.

---

3 Suian, Mihai, *Unele probleme privind folosirea probelor digitale în procesul penal,* Bucharest: Doctrina si Jurisprudenta, No. 1/2019, p. 135.

4 *Ibidem.*

5 *Ibidem.*

Featured as being a new concept of the penal trial[6], the digital evidence becomes more associated with a defensive mechanism deploying by judicial bodies who pay their attention upon digital forensic investigation. Most of the time, the digital evidence is associated with cybercrime as a new type of evidences.[7] Its main feature leads to the electromagnetic record the digital evidence exists on "easy to modify and copy, hard to understand the content directly without the conversion process, and not easy to retains the original state".[8]

The process of adapting the legislation in the field of digital evidence is an international issue[9] as a consequence the home legislation of penal procedure law is frequently out of date by the practical solutions regarding the legality of administering evidences or even investigating the crime scene in the digital area.[10]

Administering the digital evidence during the penal proceedings in Romania is strictly approached due to the fact that the new Code of penal procedure of 2014 has failed in remedying the gaps the previous penal procedural legislation was confronted with. In spite of this inconvenient, the jurisprudence reacted and identified appropriate solutions.

First of all, the judicial bodies have stated that the digital evidence is used in the penal cases having as object the serious crimes. The degree of their social danger is analyzed both from the point of view of the criminal means and *modus operandi* used by the defendants as well as from the point of view of the legal consequences produced because of

---

6 Rekhis, Slim; Boudriga, Noureddine, *Visibility: A Novel Concept for Characterizing Provable Network Digital Evidences*, International Journal of Security and Networks, No. 4/2009, pp. 234-245.

7 Sun, Jia-Rong; Shih, Mao-Lin; Hwang, Min-Shiang, *A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure,* Taichung: International Journal of Network Security, Vol. 17, No. 4/ 2015, p. 498.

8 *Ibidem*.

9 Suian, Mihai, *op. cit*., p. 135.

10 Britz, Marjie T., *Computer Forensics and Cyber Crime: An Introduction,*New Jersey: Perason Education, 2013, pp. 26-28.

the crimes committed.[11] Most of them occur in the digital environment or by technical means which involve a digital system.

Secondly, the fundamental characteristic of the general theory of administering evidence in the penal trial is that of material feature of the means of evidence. In other words, digital evidence contains trances of committing offences, but they have an immaterial character due to the fact that they exist exclusively within the digital environment. Nevertheless, the only one way for the digital evidence to be administered in the penal trial is related to the traces of committing offences which must be stocked on an information support of stocking digital data. This means that the digital evidence must be sampled from an informatics system. This activity is provided to the forensics experts in the field of the information technology.

By definition, the Code of penal procedure regulates the digital data as being "any representation of facts, information and concepts under an adequate form of processing it within an informatics system including a program which determines carrying out a function by an informatics system".[12] In accordance with the legislative definition, there are several critiques also occurred by doctrine. One of these has been pointed out by prof. Suian who stated the concept is not provided clearly enough, thus the digital data also mean "any representation of facts, information or concepts, which are recovered in an informatics system or on stocking support".[13]

Thirdly, from the procedural point of view, in order to access the information system the digital data which must be used in the penal trial are stocked on, as well as to administer them the judge's judicial authorization is necessary. The procedure is justified by the fact that through this method of forensics activity a series of encroachments in the individual's right to private life is accomplished.[14] This is a serious drawback as long as the right to the private life is established both by

---

[11] Miclea, Damian, *Cunoasterea crimei organizate,* Ploiesti: Pygmalion Publishing House, 2001, pp. 153-249.

[12] Article 138 (5) Code of penal procedure.

[13] Suian, Mihai, *op. cit.,* p. 136.

[14] Udroiu, Mihail; Slavoiu, Radu; Predescu, Ovidiu, *Tehnici speciale de investigare in justitia penala,* Bucharest: C.H. Beck Publishing House, 2009, p. 3.

the European Convention on Human Rights[15] and the European Court of Human Rights' jurisprudence.

In this respect, the European Court of Human Rights of Strasbourg pronounced several sentences against Romania because of the infringing Article 8 of the European Convention on Human Rights on respecting the right to the private life, such as Sentence of 21 April 2009: the case Raducu v. Romania[16], Sentence of 28 September 2004: the case Sabou and Pircalab v. Romania[17], Sentence of 30 June 2009: the case Burzo v. Romania[18], Sentence of 16 July 2013: the case Balteanu v. Romania[19].

The Romanian Constitution also regulate the principle of respecting the right to the private life at the Article 26 thereof which devotes the individuals' right to the private life. The public authorities are responsible for respecting the fundamental right as stated above as

---

[15] Article 8 of the European Convention on Human Rights of 1950 safeguards the individual's right to respect the private and family life and states that: "*Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*". Council of Europe, Cedex, Strasbourg. https://www.echr.coe.int/Documents/Convention_ENG.pdf

[16] Sentence of 21 April 2009 of the ECHR, available online at: https://jurisprudentacedo.com/Raducu-c.-Romaniei-Interceptare-convorbiri-telefonice-Viata-privata.html (accessed on 16 May 2019)

[17] Sentence of 28 September 2004 of the ECHR, published in the Official Journal of Romania, no. 484 of 8 June 2005, available online at: https://jurisprudentacedo.com/Sabou-si-Pircalab-contra-Romania-Interzicerea-exercitarii-drepturilor-familiale-Condamnare-penala-Conditii.html (accessed on 16 May 2019)

[18] Sentence of 30 June 2009 of the ECHR, available online at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22calmanovici%22],%22languageisocode%22:[%22RUM%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-123471%22]} (accessed on 16 May 2019)

[19] Sentence of 16 July 2013 of the ECHR, available online at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22calmanovici%22],%22languageisocode%22:[%22RUM%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-142106%22]} (accessed on 16 May 2019)

well as their family right.[20] Last but not least, the Code of penal procedure regulates at the Articles 138-153 thereof the chapter on the topic of special methods of surveillance and investigation in penal cases. Both the international and national legal framework provide the mechanism of derogation in exceptional situations.

On the one hand, the special surveillance of people exercised by the law enforcement using special technical means is considered by doctrine as being a real encroachment in their right to the private life.[21] On the other hand, the common surveillance carried out in public places regarding the individuals' activity during a short period of time does not mean entirely an encroachment in their private life as the European Court of Human Rights' jurisprudence understands to state.[22]

2. Encroachments in the individual's right to the private life

The new Code of penal procedure created *ab initio* the judicial investigation authorities' possibility to sign protocols having as object the cooperation between the investigation bodies and the intelligence services' officers. *De facto*, the last ones have been entitled to carry out specific acts of investigation by special means of technology provided outside the judge's approval. A long period of time they were into force, till the beginning of 2016 while the Constitutional Court of Romania sanctioned them and decided upon their unconstitutionality and subsequently their illegality.[23] The Constitutional Court emphasized that the systematic

---

[20] Article 26 of the Constitution of Romania republished in the Official Journal of Romania, no. 669 of 22 September 2003.

[21] Udroiu, Mihail; Slavoiu, Radu; Predescu, Ovidiu, *op. cit.*, p. 7.

[22] Sentence of 1 July 2008 of the ECHR: the case Calmanovici v. Romania, published in the Romanian Official Journal, no. 283 on 30 April 2009, available online at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22calmanovici%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-122630%22]} (accessed on 16 May 2019)

[23] Decision no. 51 of 16 February 2016 of the Constitutional Court of Romania, published in the Official Journal no. 190 of 14 March 2016, available online at: https://www.ccr.ro/files/products/Decizie_51_2016.pdf; Decision no. 244 of 6 April 2017 of the Constitutional Court of Romania, published in the

gathering of information by the intelligence services officers regarding the defendants' activity during the penal trial in particular in the investigation phase as well as recording them through the technical means of surveillance is an encroachment in the people private life. As a consequence, this kind of activity is performed through violation of the Article 8 of the European Convention on Human Rights. Actually, the Article 8 thereof permits the judicial authorities to derogate from this principle in special cases and for particular conditions expressly regulated by the Code of penal procedure. This means that the unique authority entitled to approve the technical surveillance during the investigation phase is the judge. Any other procedures parallel to the ordinary judicial procedure which would involve the other public law enforcement agencies have been declared unconstitutional. In this context, the only one question can be asked: what is happened with the judicial decisions pronounced previously which were based on these protocols? Do the decisions in penal cases produce consequences? Are they still into force? The answer cannot be a positive one due to the reason that has already stated earlier and provided by the Constitutional Court as well. The consequences of the illegal procedure adopted by the Romanian judicial authorities must be viewed in the penal procedure law's low level of quality, the lack of its clarity and precision as well as the predictability and accessibility, which all in all created the premises for infringing the defendants' procedural rights independent of their information.[24]

De iure, the encroachments exercised by the other public authorities, which are not legally entitled to carry out the investigation activity during the penal trial means a limitation of the defendants' right to private life and must be subsequently prohibited by the Constitutional Court. In these cases, it imposed a constitutional limitation in accordance with the European Convention on Human Rights' provisions and the

Official Journal no. 529 of 6 July 2017, available online at: https://www.ccr.ro/files/products/Decizie_244_2017.pdf (accessed on 16 May 2019)

[24] Selea, Mircea Mugurel, *Application of the art. 102 (2) and (3) of the Criminal Procedure Code in relation to special surveillance measures listed under the art. 138 (1) (a) and (c) of the Criminal Procedure Code enforced before the publication in the Official Journal,* Revista de Stiinte Politice, Craiova: Universitaria Publishing House, Issue no. 53/2017, pp. 104-110.

European Court of Human Rights' jurisprudence. Nevertheless, the constitutional limitation is not an absolute one, thus the defendants' surveillance can be decided by the judge in cases in which it is regulated by the penal procedure law, it is looking for a legitimate scope, it is necessary in a democratic society and it is proportionally to the proposed scope.[25]

At the international level, doctrine has also been involved in finding solutions to warrants for videotape surveillance issuable despite the lack of statutory authority.[26] On this topic, the author highlighted that the Constitution and the provisions of Code of penal procedure "*permit electronic eavesdropping by wiretaps or mechanical listening devices pursuant to a special search warrant. No constitutional or statutory authority exists, however, for the issuance of warrants permitting videotape surveillance.*"[27]

This concept also leads to the defendants' right to be informed upon request during the investigation phase on the evidence the judicial accusation is based on.[28] Knowing this feature, the defendant will be advised by his advocate regarding the legal possibilities of defense[29] as well as to combat the accusation by means of penal procedure law and propose evidence in defense. Otherwise, the restriction of defendant's procedural rights during the investigation phase will be analyzed in accordance with the European provisions.[30] Such conditions allow the European instance to appreciate the entire *de facto* circumstances of penal case as well as to restrain the infringement of the guaranteed right.[31] This is because the European Convention in particular the Article 8 thereof refers especially to the encroachments came from the public state authorities. In this matter, both doctrine and the European jurisprudence pointed out that this

---

25 Article 11 Code of penal procedure.

26 Conners, Kerry B., *Warrants for Videotape Surveillance Issuable Despite Lack of Statutory Authority,* St. John's Law Review: vol. 54, no. 4/1980, pp. 790-795.

27 *Idem*, pp. 790-791.

28 Jaidev, Ms, *Brady Ruling, 1963 U.S. Supreme Court: Sifting from being heard to open trial American and Indian Context,* International Journal of Research, vol. 05, Issue 01/2018, p. 1753.

29 Magherescu, Delia, *Recunoasterea vinovatiei si aplicarea pedepsei,* Bucharest: Hamangiu Publishing House, 2019, pp. 29-32.

30 *Idem,* p. 6.

31 Udroiu, Mihail; Slavoiu, Radu; Predescu, Ovidiu, *op. cit.,* p. 10.

principle is also applied in cases in which there are encroachments came from the natural persons upon the individuals' right as it is guaranteed by the European Convention. The syllogism consists in the fact that the state through its judicial authorities is obliged to protect their private file.[32]

Doctrine also created a particular framework on the victims' rights in criminal proceedings.[33] An antagonistic issue arose in the cases in which defendants turn into victims of the judicial authorities because of the encroachments in their private life. The dual position of the defendant, as being also a victim in the penal trial, could be viewed as an unbalance between the goals of the investigation bodies and the serious human rights violations.[34] Moreover, in the stated nexus, a paradoxical relation has been highlighted between penal trial and human rights.[35] Francoise Tulkens explains "the offensive role of human rights, which allows recourse to criminal remedies under the circumstances and conditions described above, inevitably entails other cascade effects in relation to the ECHR."[36]

Interpreting the rules of penal procedure law, the encroachments in the defendants' private life are related to those communications which are characterized by the presumption of confidentiality. From this point of view, certain theories can be advanced. One of them refers to the defendant's intimate-familial area, which exceeds common criteria which involve identifying the confidential communications. The second theory is featured in close of the defendant's nature of communications. It supposes more the subjective impact upon the defendant's right to private life violation as well as increases his status of the victim of penal trial. As it has been already pointed out above, the victimization of defendant is actually made with the public authorities' indirect consent.

---

[32] Trechsel, Stefan; Summers, Sarah J., *Human Rights in Criminal Proceedings,* Oxford: Oxford University Press, 2009, pp. 523-548.

[33] Sanchez, Juan Carlos Ochoa, *The Rights of Victims in Criminal Justice Proceedings for Serious Human Rights Violations,* Brill/ Martinus Nijhoff, 2013, pp. 71-93.

[34] *Ibidem*.

[35] Tulkens, Francoise, *The Paradoxical Relatsh between Criminal Law and Human Rights,* Journal of International Criminal Justice, vol. 9, Issue 3/2011, pp. 577-595.

[36] *Idem,* p. 591.

In opposition to the principles of the non-infringement of the defendants' procedural rights during the investigation phase[37], both theories are not exempted from criticisms. The first theory has the disadvantage of excluding from the defendants' private life their communications held in a public place, while the second one uses the subjective element which is difficult to appreciate definitely.[38] As a consequence, another criterion based on adequate theory must be provided which would determine a new feature of the presumption of confidentiality more suitable for the entire principles of penal trial.

3. Constitutional limitation

Using discretionary the means of investigation a special attention upon the digital evidence has created the reaction of the Constitutional Court which decided on the exceptions of unconstitutionality of the Code of penal procedure. In this regard, a particular feature has been created upon Article 142 (1)[39] and Article 145[40] thereof.

In relation to the first case, the Constitutional Court of Romania pronounced Decision no. 51 of 2016 on the admitting unconstitutional exception of Article 142 (1) Code of penal procedure. The Court stated that the legal provision infringe Article 1 (5) of the Constitution regarding the Romanian state, Article 20 on the international treaties regarding the human rights Romania is part of, Article 21 on the free access to justice, Article 53 on the restricting fundamental citizens' rights and liberties as well as Article 6 and Article 8 of the European Convention on Human Rights which regulate the provisions on fair trial[41] and the fundamental right on respecting private and family right. The Court also decided that the Code of penal procedure regulates expressly the

---

37 Magherescu, Delia, *op. cit*., pp. 54-55.

38 Udroiu, Mihail; Slavoiu, Radu; Predescu, Ovidiu, *op. cit.,* p. 20.

39 Decision no. 51 on 16 February 2016 of the Constitutional Court of Romania, published in the Official Journal no. 190 of 14 March 2016.

40 Decision no. 244 on 6 April 2017 of the Constitutional Court of Romania, published in the Official Journal no. 529 of 6 July 2017.

41 Magherescu, Delia, *op. cit*., pp. 21-34.

special means of investigation including the special methods of technical surveillance. Article 138 (1/a-e) Code of penal procedure enumerated those related to: intercepting the communications or any kind of long-distance communication; accessing an informatics system; video-audio surveillance; localizing or surveying by technical means; obtaining data of the persons' financial transactions. However, the Article 142 (2) Code of penal procedure states that the prosecutor does execute technical surveillance or can dispose they may be executed by the police investigation officers or by the other specialized state's bodies.

Excepting the provisions of Article 142 (1) Code of penal procedure, there is no national regulation which provides the other state's bodies to intercept or execute a technical surveillance warrant. As a consequence, such provision could be regulated only by ordinary law in a predictable and clear legal framework, but not by an "*infra-legislative legislation*"[42], such as the administrative one due to the fact that they are featured by a high degree of instability and inaccessibility. The special means of investigation are also more efficiently both for the person's involved, the defendant, for the investigation bodies and for the courts of law. Otherwise, there is the danger of infringing abusively the fundamental citizens' rights basically for the rule of law. In this regard, the constitutional standard of protecting private, family and intimate life as well as the correspondence secret impose that their limitation to be made in an appropriate legal framework which states expressly, clearly and predictably the qualified bodies to execute such activities which mean encroachments in the defendants' private life.

In accordance with the Constitutional Court's decision, the judicial bodies invested by law with such abilities are the prosecutors and the judicial police investigation bodies.[43] It does not permit to include in the Article 142 (1) Code of penal procedure provision the expression "*the other specialized state's bodies*" which are not defined or specified within the Code or another ordinary law.

---

[42] Decision no. 51 on 16 February 2016 of the Constitutional Court of Romania, published in the Official Journal no. 190 of 14 March 2016.

[43] In conformity with Article 30 Code of penal procedure corroborated with Article 55 (5) thereof.

The second case occurs on the Constitutional Court Decision no. 244/2017 regarding the unconstitutional exception of Article 145 Code of penal procedure invoked in Case no. 4821/1/2015 in front of the High Court of Cassation and Justice which opined that the technical surveillance included means of evidence that supposed serious encroachments in the defendant's private life, right already protected by Article 26 and 28 of the Romanian Constitution. The High Court of Cassation and Justice appreciated that the verification of these means of investigation legality could be done exceptionally by incidental way in particular cases. In this context, the supreme court stated there is no legal provision which permits defendants to request the verification of legality of administering evidence in accordance with Article 340 Code of penal procedure.

Constitutional Court emphasized that the unconstitutional exception invoked referred to the "rights and liberties judge's conclusion pronounced on the means of technical surveillance cannot be appealed". For this reason, the parties involved in a penal trial cannot appeal the conclusion pronounced by the judge of rights and liberties on the means of technical surveillance. The Court's jurisprudence states that in principle the measure infringe the defendant's procedural right or a legitimate interest he is entitled to intimate the court of law in order to invoke the damage suffered and remove it even if the procedure implies exercising appeal. As pointed out by the European Court of Human Rights' jurisprudence, from the point of view of the legal nature, the right to appeal provided by Article 13 European Convention of Human Rights is a subjective procedural right which guarantees the access to justice in front of the court of law that may reestablish the legal situation.

Regarding the case of Romania, the Court's decisions highlight that its jurisprudence in the matter of process remedy against the means of technical surveillance has known an evolution during the last period of time. Initially, the European Court of Human Rights observed that, in accordance with the home law, a person whose legitimate interests have been infringed by using technical means of investigation could request the court of law to declare illegality of the means of intercepting the private communications and obtain

compensations[44]. Subsequently, the European Court of Human Rights stated that Romania did not provide an example of the law courts' jurisprudence which demonstrates the appeal efficiency in this matter. Moreover, the Court also stated that the civil appeal declared by entitled person to involve the state's responsibility in order to obtain compensations does not permit a control of legality of intercepting the private communications and a decision to dispose destroying them. This means that there is no effective control in accordance with Article 8 of the Convention.

In conclusion, in the field of the technical means of surveillance that really mean an encroachment in the defendants' private life, an *a posteriori* control can exist in purpose to verify the legal conditions regulated and the modality of executing the technical surveillance warrant, as provided by Article 142-144 Code of penal procedure. Both the constitutional and European jurisprudence impose the positive state's obligation having as object the regulation of "effective appeal" which allows removing possible infringements of the defendants' fundamental rights and liberties. It is appreciated that in absence of such an appeal in the penal proceedings means a violation of the obligation, in particular of the Article 21 of the Constitution and Article 13 of the European Convention.

Doctrine also has been involved in how these provisions suppose changing the nature of the defendants' presumption of innocence while they are surveyed and how the legislator can rewrite the human rights and regulate the use of surveillance technologies in such a matter not to imply an encroachment in the defendants' private life.[45] The author points out that "the widespread use of surveillance technologies and their huge technological potential emphasize the need to focus on the relationship between surveillance and the presumption of innocence.

---

[44] Sentence of 16 July 2013 of the ECHR: Case Balteanu v. Romania, available online at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22calmanovici%22],%22languageisocode%22:[%22RUM%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-142106%22]} (accessed on 16 May 2019)

[45] Galetta, Antonella *The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?,* Belfast: European Journal of Law and Technology, Vol. 4, No. 2/2013.

The link between surveillance and the presumption of innocence is very close, considered that surveillance measures are deployed to control, detect, deter and prevent crime."[46]

As a consequence, using the special means of technological investigation by inappropriate state's bodies other than the judicial ones turns into the erosion of the defendants' presumption of innocence during the penal proceedings[47] especially in cases in which the secret services use this kind of technology in executing the prosecutor's decision.

4. Particularities of the procedure involving digital investigation

The procedure in penal cases of digital investigation involves priory the informatics or digital search and the investigation of the "*crime scene*" of the informatics offences. The legal basis of the digital search is provided by the Code of penal procedure, Article 168 thereof. It is a conclusive forensic method which consists in investigating a digital system or a support that stocks information data in purpose to find and gather digital evidence necessary in solving the penal cases. The main purpose of digital search is given by drawing digital evidence – electronic information having conclusive value, preserving the digital data which contain traces of informatics offences in those cases in which there is the danger of losing or modifying them.

The penal procedure of digital search presents the following characteristics:

- It represents a special technique of forensic investigation in criminal matters. Doctrine has appreciated the digital search alongside with accessing a digital system, regulated by Article 138 (1/b) and (3) Code of penal procedure represents encroachments in the defendants' right to the private life, as it has been already pointed out in the previous section of the current paper. The procedure neither involves the penetration of the defendants' domicile, nor excludes it. In accordance with the previous penal

[46] *Ibidem*.

[47] *Ibidem*.

procedural regulation, provided by Law no. 161/2003, the digital search was disposed beforehand taking the digital system within the domiciliary search.

- The necessity to protect the defendants' private life directs to imposing some additional guarantees in cases of digital search. The legislator has stated in such cases applying the same guarantees as in cases of domiciliary search.

- The digital search is disposed in cases in which there are reasonable reasons for the investigation bodies to consider that the digital system or the support of stocking the digital data that is subject to the digital search contains digital evidence regarding the offence committed and the judicial measure is necessary and proportional to the proposed judicial purpose.

Article 168 (1) Code of penal procedure regulates "digital system search or a support of stocking the digital data means the investigation method of discovering, identifying and gathering digital evidence stocked in a digital system materialized through technical means and adequate proceedings of assuring the integrity of such information therein".

During the investigation phase, the competence in disposing the procedure of digital search belongs to the judge of rights and liberties who can admits the prosecutor's request of carrying out the digital search. Procedural speaking, the prosecutor submits his request with the penal case to the judge of rights and liberties, who will decide immediately in the council room in the presence of the prosecutor. In cases in which the judge considers the request is founded will admit it and dispose allowing the digital search through issuing the search warrant. The decision is definitively and cannot be subject to appeal.

The search warrant contains the legal elements, as provided by the Code of penal procedure. They consist in mentioning the scope it has been issued for; the digital system or the support of stoking the digital data which must be searched; the defendant's name if known.

A particular situation could be arisen in cases of digital search. There is the possibility for the forensic investigators to find that the digital data the forensic investigators look for are contained by another digital system which can be accessed from the initial system. In this case, the prosecutor disposes immediately the preserving and copying them. The procedure requires the prosecutor will solicit completing the search warrant on the new digital system.

In those cases of carrying out digital search the investigation bodies must pay a special attention on this procedure including the number and size of digital system, the nature of wireless network and internal network as well in order to maintain unimpaired the digital data content. In this sense, the digital evidence will not be distorted or even modified. The detailed procedure of carrying out the digital search is provided by the Introductory Guide of Applying Legal Regulations regarding the Digital Criminality, drawing up by the Ministry of Communications and Information Technology[48] in 2004.[49] It provides aspects regarding the procedure of taking the digital system, shutting down the system, labeling the components, protecting against the data modification as well as transporting them to the laboratory.

Within the digital search the forensic investigators will proceed to copying the digital data gathered from the digital system. It is advisable for the investigation bodies to proceed in double-sample copy, one of them will be sealed as a witness-evidence, and another one will be used in purpose to extract the digital data. The memory supports the digital data are copying on as well as the envelopes they are introduced in will be signed by the forensic investigators who participated in the digital search.

Despite the penal procedure of digital search, the interest occurs on the person entitled to carrying out it. The code of penal procedure regulates that the competence in carrying out the digital search belongs to the forensic investigator that is working within the judicial bodies. The activity of digital search is made in the presence of the prosecutor.

5. Jurisprudential references

Case 1:

Once the Constitutional Court pronounced on the illegal use of defendants' surveillance technologies by the other state's bodies than the judicial ones, the courts of law in penal matters were entitled to decide

[48] The Introductory Guide of Applying Legal Regulations regarding the Digital Criminality, Bucharest: INTERNEWS RITI dot-GOV, 2004.

[49] Olteanu, Gabriel Ion; Ruiu, Marin, *Tactica criminalistica,* Bucharest: AIT Laboratories Publishing House, 2009, pp. 142-146.

upon the illegality of such administrative measures. Regarding this aspect, the law courts' jurisprudence is very rich in decisions pronounced in cases in which such illegal surveillance technologies were used.

Considering the fundamental principles of respecting private life and human rights entirely, the activity of investigation carrying out through infringing the defendant's rights supposes the nullity of such activity. Regarding the principle of administering digital evidence they must be gathered through respecting legal provisions.[50] During the pre-trial court the defendant has formulated exceptions on the legality of administering digital evidence as well as on carrying out the activity of the investigation phase by the General Prosecutor Office attached to the High Court of Cassation and Justice – Direction of the Investigating Organized Crimes and Terrorism. The judge of preliminary court understood that the defendants were sent to trial due to committing the offence of initiating an organized criminal group incriminated by Article 367 (1) and (2) penal Code, offence of trafficking of minors incriminated by Article 211 (1) and (2) penal Code and trafficking of human beings also incriminated by penal Code at the Article 210 (1/a and b) thereof.

The prosecutor retained the fact that during the period of time between 2011 and 2016 the defendants set up an organized criminal group which was involved in "recruiting, transporting, accommodating and sexual transnational exploiting of 5 minor women between the age of 15 and 17 years old and a number of 24 major women which came from disadvantaged families having a low level of education, with a very precarious material situation and different vulnerabilities".[51]

The prosecutor also stated in the indictment act that the group's leader coordinated and surveyed entire criminal operation consisting in the women' sexual exploitation which took place in Italy. The women were allured through the pretext of being engaged in well-paid labors in the destination country where they will receive a huge salary. Actually, the entire amount of money proceeded from criminal activities were sent in the defendants' home country and distributed among the group

[50] Penal Decision no. 18 of 15 February 2017 of the Court of Law of Iasi, available online at: http://portal.just.ro/99/Lists/Jurisprudenta/DispForm.aspx?ID=378

[51] *Ibidem*.

members. It has been established that during the period between 2011 and 2015, an amount of 28.165 Euros was sent in Romania via Western Union services. The amount collected by defendants constitutes the proceeds of crime committed by themselves in Italy.

De facto situation is proved through evidence gathered by technical means and administered in the penal case. The defendants invoked the exception of illegality of the investigation activities argued that they are illegal both from the point of view of the offence retained by prosecutor and their concordance with the act of indictment. On the one hand, regarding the illegal feature of the evidence administered in the penal case, the defendants requested from the judge of pre-trial court returning the case to the investigation phase as well as establishing nullity of the acts of intercepting private telephone calls due to the fact that, in accordance with the Constitutional Court decision no. 51/2016, they were carried out by the Romanian Service of Intelligence.

The defendants admitted during the investigation phase the court of law authorized actions of intercepting their telephone calls, but they were carried out by another state body than the investigation one. For this reason, the only one sanction applied for those actions is the nullity of the procedural acts carried out in such circumstances. This means that the evidence gathered by digital means of technical surveillance is null.

Considering from the constitutional point of view, the defendants emphasized that in the penal case Article 11 (2) Code of penal procedure on respecting the human dignity and private life was infringed. The pre-trial judge appreciated that the role of this procedure is that of verifying the legality of evidence administered which "institutes the pre-trial judge's competence to verify the conformity of evidence administered during the investigation phase with the guarantees of the procedure fairness."[52]

The pre-trial judge stated there are vices of illegality. In this matter, the judge admitted the defendants' right to defense has been respected with its entire legal elements. They have been also informed on the offence committed the indictment act is based on as well as the offences legal integration, as premises for the fair trial.

---

[52] *Ibidem*.

Regarding the principle of legality and loyalty of administering evidence during the investigation phase, the pre-trial judge stated that the actions of technical surveillance lead with the Constitutional Court's decision and provision of Article 102 (3) Code of penal procedure due to the fact that they were carried out by another administrative body instead of the judicial one. Taking into account this aspect, the pre-trial judge stated that the defendants "indicated concretely neither what kind of interceptions they invoked the illegality with not what kind of nullity would affect these interceptions as being illegal ones in accordance with the Constitutional Court Decision no. 51/2016 they are prevailed with".[53]

Case 2:

In accordance with the Constitutional Court Decision no. 302/2017[54] the legislative solution regulated by Article 281 (1/b) Code of penal procedure which does not provide the sanction of nullity in cases of infringing provisions regarding the investigation bodies' procedural competence *rationae persone* and *rationae materie* was declared unconstitutionally. Moreover, infringing provisions on executing procedural measures of technical surveillance including the other specialized state bodies' technical support is sanctioned by absolute nullity.

De iure, the pre-trial judge of the High Court of Cassation and Justice admitted the defendant's request and pre-trial exceptions regarding the illegality of the indictment act issued by the General Prosecutor Office attached to the High Court of Cassation and Justice – The National Anticorruption Directorate regarding the offences description and their legal integration as well as regarding the means of evidence administered.[55]

---

[53] *Ibidem*.

[54] Decision no. 302 of 4 May 2017 of the Constitutional Court on the exception of unconstitutionality of Article 281 (1/b) Code of penal procedure, available online at: https://ccr.ro/files/products/Decizie_302_2017.pdf (accessed on 22 May 2019)

[55] Conclusion no. 31/C of 27 September 2018 of the High Court of Cassation and Justice, available online at: https://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=147655 (accessed on 24 March 2019)

The indictment act contains the prosecutor's decision on the defendant's procedural status of being sent to trial for committing the tax evasion offence incriminated by Article 9 (1/c) and (3) of Law no. 241/2005[56] and carrying out illegal financial operations as commercial activities by an incompatible person, incriminated by Article 12 (a) of Law no. 78/2000[57].

The defendant appealed the pre-trial judge's conclusion arguing the fact that the fair trial principle is guaranteed through administering legal evidence. Moreover, defendant criticized the modality of administering evidence in the investigation phase from the point of view of the measures of technical surveillance illegality as exception also invoked by defendant.

The court of law observed that technical measures of surveillance having as object intercepting and recording telephone calls and communications as well as intercepting and audio-video recording the conversations discussed in the ambient environment and localizing and surveying by GPS were authorized in accordance with Article 138 Code of penal procedure. Initially, the provisions of Article 142 (1) Code of penal procedure regulates that "the prosecutor executes the technical surveillance order or can dispose it can be carried out by the investigation police body or specialized police officers or by the other state's specialized bodies". Once the Constitutional Court decision no. 51/2016 entered into force the legal expression "or by the other state's specialized bodies" is unconstitutional.

The court of law admitted the defendant's request and disposed to the Prosecutor Office to specify "what the public authority executed the technical surveillance warrant in the current penal case and the implication of the Romanian Intelligence Service in the investigation activities, more particular what kind of these activities were carried out by the last institution".[58] The prosecutor issued the official response which stated that the technical surveillance warrants disposed by the competent court

---

[56] Law no. 241/2005 on preventing and combating tax evasion, published in the Official Journal no. 672 of 27 July 2005.

[57] Law no. 78/2000 on preventing, discovering and sanctioning offences of corruption, published in the Official Journal no. 219 of 18 May 2000.

[58] Conclusion no. 31/C of 27 September 2018 of the High Court of Cassation and Justice, available online at: https://www.scj.ro/1093/Detalii-jurisprudenta?

of law have been executed with the technical support of the Romanian Intelligence Service "but the procedural reports of registering the results of technical surveillance activities have been drawn up in accordance with Article 143 Code of penal procedure by the judicial police officers within the Anticorruption National Directorate ."[59]

Regarding the current investigation activity, it has been argued that the provisions of the Article 142 (1) Code of penal procedure were into force at the moment of disposing the special measures of technical surveillance both in the beginning and at the end of these activities. At the same time, the prosecutor pointed out that although the Romanian Intelligence Service was involved in the technical surveillance activities it did not carry out investigation activity during the investigation phase.

Taking into account the constitutional limitation in the penal case the legal provisions on carrying out the measures of technical surveillance have been infringed due to the fact that these activities were fulfilled by a state body having no competence in carrying out activities of investigation procedure. The situation produces the infringement of competence regulations that is sanctioned by absolute nullity. Moreover, in accordance with the Constitutional Court decision no. 302/2017 infringing the provisions of investigation bodies' competence is also sanctioned by absolute nullity, its legal effects being regulated by Article 281 Code of penal procedure.

Considering all these aspects stated above, the court of law decided removing the means of evidence and the supports that contain the result of the means of technical surveillance existed in the penal trial. At the same time, it stated removing all aspects related to these means of evidence and their content. For these reasons, the court of law admitted the defendant's appeal, repealed the conclusions invoked and declared the absolute nullity of the measures of technical surveillance. In accordance with Article 102 (2-4) Code of penal procedure, the court of law decided

customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=147655 (accessed on 24 March 2019)

[59] *Ibidem*.

to remove the procedural reports of registering the results of technical surveillance activities from the penal case.[60]

Conclusions

The criminality committed within the digital environment is the social phenomenon which refers to the diversity of criminal acts and activities the perpetrators commit. From a substantive penal law point of view, protecting such environment is carried out by special means of digital security.[61] Nevertheless, in the field of penal procedure law a particular regulation regarding the serious crimes is also necessary.

At present, the provisions regulated by the Code of penal procedure in Romania still creates difficulties in the judicial bodies' activity of achieving the scope of the penal trial consisting in finding the judicial truth based on legal evidence. The serious drawbacks existed in the judiciary must be corroborated with the constitutional limitation imposed on the illegal procedure of gathering digital evidence carried out by the other state's bodies than the investigation ones.

Taking into account these aspects, a set of *de lege ferenda* proposals has been identified and advanced in purpose to improve the legal framework of solving the cases in criminal matters.

Basically, having in view the major deficiencies of the penal procedure legislation into force, the proposals refer to the following aspects.

It is obviously that committing serious crimes[62], a special aggravated procedure is imperatively to be implemented in the justice

---

[60] For the similar reference, see also Conclusion no. 31/C of 27 September 2018 of the High Court of Cassation and Decision, available online at: https://www.scj.ro/1094/Detalii-dosar?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=100000000316375

[61] Alecu, Gheorghe; Barbaneagra, Alexei, *Reglementarea penală și investigarea criminalistică a infractiunilor din domeniul informatic,* Bucharest: Pinguin Book Publishing House, 2006, pp. 188-215.

[62] Gounev, Philip; Ruggiero, Vincenzo, *Corruption and Organized Crime in Europe. Illegal Partnerships,* London and New York: Routledge Taylor and Francis Group, 2012, pp. 4-12; Campana, Paolo, *Understanding Then Responding*

in criminal matters[63], this kind of crimes to be solved on. The special procedure must be derogatory regulated from the ordinary penal procedure. It must regulate both the investigation and the judgment phases of penal trial. During the investigation phase, the main activity should take into account approaching the procedure of achieving:

- investigation of serious crimes, under the special aggravated procedure;

- aspects regarding the discovering, identifying, preserving, analyzing and administering digital evidence.

Among these activities, the legislator must focus its attention to administering digital evidence in order to regulate and implement it in the penal trial due to the fact that at present the Romanian legislation in criminal matters does not recognize *de lege lata* the possibility of administering digital evidence directly during the penal proceedings.[64]

References

ALECU, Gheorghe; BARBANEAGRA, Alexei, *Reglementarea penală și investigarea criminalistică a infractiunilor din domeniul informatic,* Bucharest: Pinguin Book Publishing House, 2006.

BRITZ, Marjie T., *Computer Forensics and Cyber Crime: An Introduction,* New Jersey: Perason Education, 2013.

CAMPANA, Paolo, *Understanding Then Responding to Italian Organized Crime Operations across Territories*, Policing: A Journal of Policy and Practice, Vol. 7, Issue 3/2013, pp. 316-325, https://doi.org/10.1093/police/pat012

CONNERS, Kerry B., *Warrants for Videotape Surveillance Issuable Despite Lack of Statutory Authority,* St. John's Law Review: vol. 54, no. 4/1980, available online at: https://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=2418&context=lawreview (accessed on 18 May 2019)

to Italian Organized Crime Operations across Territories, Policing: A Journal of Policy and Practice, Vol. 7, Issue 3/2013, pp. 316-325.

63 Dusek, Libor, *Time to punishment: The effects of a shorter criminal procedure on crime rates,* International Review of Law and Economics, Vol. 43/2015, pp. 134-147.

64 Suian, Mihai, *op. cit.,* p. 136.

CONSTITUTION OF ROMANIA republished in the Official Journal of Romania, no. 669 of 22 September 2003, Bucharest: Themis Publishing House, 2003.

CONSTITUTIONAL COURT DECISIONS, Jurisprudence of admitting decisions, available online at: https://www.ccr.ro/jurisprudenta-decizii-de-admitere (accessed on 17 May 2019)

DUSEK, Libor, *Time to punishment: The effects of a shorter criminal procedure on crime rates,* International Review of Law and Economics, Vol. 43/2015, https://doi.org/10.1016/j.irle.2014.04.007

GALETTA, Antonella *The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?,* Belfast: European Journal of Law and Technology, Vol. 4, No. 2/2013, available online at: http://ejlt.org/article/view/221/377 (accessed on 14 May 2019)

GOUNEV, Philip; RUGGIERO, Vincenzo, *Corruption and Organized Crime in Europe. Illegal Partnerships,* London and New York: Routledge Taylor and Francis Group, 2012.

INTRODUCTORY GUIDE of Applying Legal Regulations regarding the Digital Criminality, Bucharest: INTERNEWS RITI dot-GOV, 2004, available online at: http://www.riti-internews.ro/ro/ghid.htm (accessed on 17 May 2019).

JAIDEV, Ms., *Brady Ruling, 1963 U.S. Supreme Court: Sifting from being heard to open trial American and Indian Context,* International Journal of Research, vol. 05, Issue 01/2018, available online at: https://journals.eduindex.org/index.php/ijr/article/view/11807/11144 (accessed on 16 May 2019)

JURISPRUDENTA CEDO of Strasbourg, European Court of Human Rights, 2019. https://jurisprudentacedo.com/respectarea-vietii-private-si-familiale.html

LAW NO. 135/2010 on the Code of penal procedure of Romania, published in the Official Journal of Romania, no. 486 of 15 July 2010, entered into force on February 1, 2014.

MAGHERESCU, Delia, *Recunoasterea vinovatiei si aplicarea pedepsei,* Bucharest: Hamangiu Publishing House, 2019.

MICLEA, Damian, *Cunoasterea crimei organizate,* Ploiesti: Pygmalion Publishing House, 2001.

OLTEANU, Gabriel Ion; RUIU, Marin, *Tectica criminalistica,* Bucharest: AIT Laboratories Publishing House, 2009.

REKHIS, Slim; BOUDRIGA, Noureddine, *Visibility: A Novel Concept for Characterizing Provable Network Digital Evidences*, International Journal of Security and Networks, No. 4/2009, available online at: https://www.researchgate.net/publication/220080823_Visibility_A_novel_concept_for_characterising_provable_network_digital_evidences (accessed on 21 May 2019)

SANCHEZ, Juan Carlos Ochoa, *The Rights of Victims in Criminal Justice Proceedings for Serious Human Rights Violations,* Brill/ Martinus Nijhoff, 2013.

SELEA, Mircea Mugurel, *Application of the art. 102 (2) and (3) of the Criminal Procedure Code in relation to special surveillance measures listed under the art. 138 (1) (a) and (c) of the Criminal Procedure Code enforced before the publication in the Official Journal,* Revista de Stiinte Politice, Craiova: Universitaria Publishing House, Issue no. 53/2017, available online at: https://cis01.central.ucv.ro/revistadestiintepolitice/files/numarul53_2017/10.pdf (accessed on 21 May 2019).

SUIAN, Mihai, *Unele probleme privind folosirea probelor digitale in procesul penal.* Bucharest: Doctrina si Jurisprudenta, No. 1/2019.

SUN, Jia-Rong; SHIH, Mao-Lin; HWANG, Min-Shiang, *A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure,* Taichung: International Journal of Network Security, Vol. 17, No. 4, 2015, available online at: http://ijns.jalaxy.com.tw/contents/ijns-v17-n5/ijns-2015-v17-n5-p497-509.pdf (accessed on 21 May 2019).

TRECHSEL, Stefan; SUMMERS, Sarah J., *Human Rights in criminal Proceedings,* Oxford: Oxford University Press, 2009.

TULKENS, Francoise, *The Paradoxical Relationship between Criminal Law and Human Rights,* Journal of International Criminal Justice, vol. 9, Issue 3/2011, https://doi.org/10.1093/jicj/mqr028

UDROIU, Mihail; SLAVOIU, Radu; PREDESCU, Ovidiu, *Tehnici speciale de investigare in justitia penala,* Bucharest: C.H.Beck Publishing House, 2009.

Informações adicionais e declarações dos autores
(integridade científica)

Agradecimentos (acknowledgement): I would like to express my thanks to those professionals who helped me in carrying out the final version of my article, including the anonymous reviewers as well as the RBDPP Editorial Board who evaluated and accepted it in order to be published in the journal 2019 Special Issue.

Declaração de conflito de interesses (conflict of interest declaration): the author confirms that there are no conflicts of interest in conducting this research and writing this article.

Declaração de autoria e especificação das contribuições (declaration of authorship): all and only researchers who comply the authorship requirements of this article are listed as authors; all co-authors are fully responsible for this work in its entirety.

Declaração de ineditismo e originalidade (declaration of originality): the author assures that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; she also attests that there is no third party plagiarism or self-plagiarism.

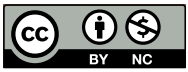
Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 11/06/2019
- Controle preliminar e verificação de plágio: 23/07/2019
- Avaliação 1: 27/07/2019
- Avaliação 2: 12/08/2019
- Decisão editorial preliminar: 26/09/2019
- Retorno rodada de correções: 29/09/2019
- Decisão editorial final: 29/09/2019

Equipe editorial envolvida
- Editor-chefe: 1 (VGV)
- Editora-associada: 1 (CC)
- Revisores: 2

COMO CITAR ESTE ARTIGO:

MAGHERESCU, Delia. Using New Means of Technology during the Penal Proceedings in Romania. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1189-1217, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.250



Las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales

Videoconferencing of inmates with the defence lawyer or with the lawyer expressly called in relation to criminal matters

Pablo García Molina[1]

Universidad de Cádiz – Cádiz/España

pablo.garciamolina@uca.es

http://orcid.org/0000-0003-2101-8472

Resumen: El uso de la videoconferencia en la Administración de Justicia española, y, más concretamente, en el proceso penal español, no es algo novedoso, ni siquiera en los centros penitenciarios, donde desde hace más de una década se hace uso de esta tecnología para facilitar la práctica de algunas actuaciones judiciales. Sin embargo, su uso para otros fines es completa o prácticamente inexistente, a pesar de que puede ser muy adecuada, entre otras cosas, para facilitar las comunicaciones entre el interno y sus familiares, para que se le preste al interno asistencia médica, o para las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales. Precisamente, este trabajo se centra en esta última posibilidad al analizar si actualmente este tipo de comunicaciones está regulada o no en la normativa penitenciaria española, si existen antecedentes al respecto en nuestro país, qué ventajas y deseventajas presenta, cómo ha de desarrollarse y qué garantías debe tener.

Palabras-clave: comunicaciones; videoconferencia; internos; abogado.

Abstract: *The use of videoconferencing in the Spanish Administration of Justice,*

[1] Profesor Sustituto Interino de Derecho Procesal de la Universidad de Cádiz.

and more specifically, in the Spanish criminal process, is not something new, not even in prisons, where for more than a decade this technology has been used to facilitate the practice of some judicial proceedings. However, its use for other purposes is complete or practically non-existent, although it may be very appropriate, among other things, to facilitate communications between the inmate and his family, to provide the inmate with medical assistance, or for videoconferencing of inmates with the defence lawyer or with the lawyer expressly called in relation to criminal matters. Precisely, this work focuses on the latter possibility when analysing whether this type of communication is currently regulated or not in the Spanish penitentiary regulations, if there are antecedents in this respect in our country, what advantages and disadvantages does it present, how it must be developed and what guarantees it must have.

Keywords: *communications; videoconferencing; inmates; lawyer.*

Introducción

La videoconferencia es un sistema que permite la comunicación bidireccional y simultánea de la imagen y el sonido y la interacción visual, auditiva y verbal entre dos personas o grupos de personas geográficamente distantes (arts. 229.3 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial [en adelante, LOPJ] y 325 y 731 bis. del Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal [en adelante, LECrim])[2].

La idea original del uso de la videoconferencia en los centros penitenciarios era facilitar la práctica de diligencias de investigación y la celebración de juicios orales, idea en torno a la cual, como veremos

[2] El Diccionario de la lengua española define la palabra videoconferencia como la "comunicación a distancia entre dos o más personas, que pueden verse y oírse a través de una red".

a continuación, se ha desarrollado el uso de esta tecnología en la Administración de Justicia[3].

Así, por ejemplo, cabría hacer uso de la videoconferencia para la práctica de algunas actuaciones judiciales que se desarrollan durante la instrucción o el juicio oral como, por ejemplo, para celebrar ruedas de reconocimiento[4]; vistas de prórrogas de prisión[5]; algunas diligencias de prueba en el juicio oral; o, incluso, para las entrevistas de los fiscales,

---

[3] Para una panorámica general sobre el uso de la videoconferencia en la Administración de Justicia española vid. GUTIÉRREZ BARRENENGOA, Ainhoa. La utilización de la videoconferencia en la Administración de Justicia. En: HERRÁN ORTIZ, Ana Isabel; EMALDI CIRIÓN, Aitziber; ENCISO SANTOCILDES, Marta (Eds.), *Derecho y Nuevas Tecnologías*. Bilbao: Universidad de Deusto, 2010. v. 2, p. 121-134; y VALBUENA GONZÁLEZ, Félix. Proceso penal y videoconferencia. En: HERRÁN ORTIZ, Ana Isabel; EMALDI CIRIÓN, Aitziber; ENCISO SANTOCILDES, Marta (Eds.), *Derecho y Nuevas Tecnologías*. Bilbao: Universidad de Deusto, 2010. v. 3, p. 83-95.

[4] Vid. la Sentencia 669/2017, de 11 de octubre, de la Sección 1ª de la Sala de lo Penal del Tribunal Supremo, y la Sentencia 211/2016, de 29 de abril, de la Sección 3ª de la Audiencia Provincial de Córdoba, en las que se narran sendos casos en los que se realizan ruedas de reconocimiento a través de videoconferencia con el centro penitenciario. En contra del uso de esta tecnología, en este caso, en relación con un sujeto que se encontraba en libertad, se pronuncia el Auto 536/2015, de 23 de diciembre, de la Sección 3ª de la Audiencia Provincial de Cantabria, según el cual, "de pretenderse situar a todas las personas que formasen la rueda en una sala de vistas y proceder desde allí al reconocimiento por videoconferencia, existiría el óbice de tener que utilizar grandes angulares para recoger al mismo tiempo la imagen de todas las personas que conformasen la rueda, lo que supondría minimizar sus imágenes, con la posibilidad de visionado irregular de sus características físicas, al estar las personas a una gran distancia focal del objetivo -la relativización de las dimensiones a la que se refiere el Juez instructor en el auto resolutorio del previo recurso de reforma-. Y siempre podría alegar el Letrado defensor del recognoscible que no ha estado presente en el otro punto de la videoconferencia [...], que no ha podido observar si se veía o no bien a los recognoscibles y que no ha podido acotar preguntando al recognosciente lo que estimara procedente sobre la persona reconocida, postulando después la nulidad de la prueba. Pero es que, a mayor abundamiento, aunque hubiere sistemas que permitieran un visionado claro y amplio de las personas a reconocer, siempre será competencia del juez instructor y del Letrado/a de la Administración de Justicia del Juzgado la conformación de la rueda y la supervisión de la práctica de la diligencia".

[5] Esto ha sido utilizado por la Audiencia Provincial de Alicante en diversas ocasiones.

de menores o de adultos; y de los jueces, de menores o de vigilancia penitenciaria, con los internos en un centro de internamiento de menores infractores o en un centro penitenciario[6]. Todos estos casos tienen en común que uno de los sujetos que intervienen en la comunicación (concretamente, el sujeto pasivo del proceso penal) se encontraría interno en un centro penitenciario como preso preventivo o como penado, mientras que el resto de los intervinientes (juez, letrado de la Administración de Justicia, fiscal, abogados, testigos, peritos, etc.) se encontrarían fuera del mismo.

Sin embargo, su uso para otros fines es completa o prácticamente inexistente, a pesar de que puede ser muy adecuado, entre otras cosas, para facilitar las comunicaciones entre el interno y sus familiares, para que se le preste al interno asistencia médica, o para las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales, lo que contribuiría a garantizar el ejercicio del derecho a la defensa y a la asistencia de letrado, finalidad que, aunque actualmente no está prevista

---

[6] El Plan de Implantación del Sistema de Videoconferencia del Ministerio de Justicia de 4 de diciembre de 2001, preveía entre los usos del sistema de videoconferencia para la Administración de Justicia las entrevistas de los Jueces de Vigilancia Penitenciaria con los reclusos. Más recientemente, el art. 675 de la Propuesta de texto articulado de Ley de Enjuiciamiento Criminal de 2013, preveía expresamente que el interno en un centro penitenciario, cumpliendo condena o en situación de prisión preventiva, tenía derecho al menos cada tres meses a mantener una entrevista personal o mediante videoconferencia con el titular del Tribunal de Vigilancia Penitenciaria. La posibilidad de que el contacto pueda facilitarse a través de videoconferencia se recoge expresamente en la página web de la Secretaría General de Instituciones Penitenciarias, disponible en http://www.iipp.es/web/portal/laVidaEnPrision/derechosDeberes/Derechos/juzgadoVigilancia.html (consultado el 1 de julio de 2019). Asimismo, el Plan de Implantación del Sistema de Videoconferencia del Ministerio de Justicia de 4 de diciembre de 2001, preveía entre los usos del sistema de videoconferencia para la Administración de Justicia, entre otras cuestiones, las entrevistas a menores en centros de internamiento por las Fiscalías o Juzgados de Menores. Más recientemente, la Instrucción 3/2002, de 1 de marzo, de la Fiscalía General del Estado, sobre actos procesales que pueden celebrarse a través de videoconferencia, preveía la posibilidad de utilizar la videoconferencia para actos no estrictamente procesales (v. gr. la entrevista del Fiscal con internos en centros penitenciarios).

en nuestra normativa penitenciaria, entendemos necesaria[7], motivo por el cual la estudiaremos a continuación con detalle en este trabajo.

En este sentido no hemos de olvidar que los considerandos 23 y 44 de la Directiva 2013/48/UE del Parlamento Europeo y del Consejo de 22 de octubre de 2013 sobre el derecho a la asistencia de letrado en los procesos penales y en los procedimientos relativos a la orden de detención europea, y sobre el derecho a que se informe a un tercero en el momento de la privación de libertad y a comunicarse con terceros y con autoridades consulares durante la privación de libertad, dicen que tanto los sospechosos o acusados como las personas reclamadas deben tener derecho a comunicarse con el letrado que los represente. Esta comunicación puede tener lugar en cualquier momento del proceso, inclusive antes de ejercer el derecho a reunirse con el letrado. Los Estados miembros pueden adoptar disposiciones prácticas sobre la duración, la frecuencia y los medios de dicha comunicación, incluido el uso de la videoconferencia y otras tecnologías de la comunicación con el fin de que pueda tener lugar tal comunicación, siempre que dichas disposiciones prácticas no vayan en detrimento del ejercicio efectivo ni del contenido esencial del derecho de esas personas a comunicarse con sus letrados.

Esta Directiva fue traspuesta al Derecho interno por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, que, aunque ha dado lugar a algunos avances en relación con el ejercicio del derecho a la defensa y a la asistencia de letrado[8], no prevé expresamente el uso de la videoconferencia u otras tecnologías de la comunicación para que tanto los sospechosos o acusados como las personas reclamadas puedan ejercer su derecho a

---

7 En el mismo sentido se pronuncia JORDÁN DÍAZ-RONCERO, María José. *Análisis de la implantación y eficacia de la videoconferencia en el proceso penal español: hacia una modernización de nuestro sistema de justicia penal*. Tesis Doctoral (Programa de Doctorado en Derecho, Empresa y Justicia) – Universidad de Valencia, Valencia, 2014, p. 471. Disponible en: <http://roderic.uv.es/handle/10550/44107>. Consultado el: 1 jul. 2019.

8 Como, por ejemplo, lo dispuesto en el art. 520.2.c) LECrim, que prevé que, en caso de que, debido a la lejanía geográfica no sea posible de inmediato la asistencia de letrado, debe facilitarse al detenido comunicación telefónica o por videoconferencia con aquel, salvo que dicha comunicación sea imposible.

comunicarse con el letrado que los represente en cualquier momento del proceso a través de estos medios mientras se encuentren internos como presos preventivos o penados en un centro penitenciario.

1. Regulación

La implantación de la videoconferencia en la Administración de Justicia española se produjo a partir del año 2002 y se vio reflejada en la Ley Orgánica 13/2003, de 24 de octubre, de reforma de la Ley de Enjuiciamiento Criminal en materia de prisión provisional, que se aprovechó para introducir esta tecnología de forma expresa en el proceso. No obstante, ello no quiere decir que anteriormente no se utilizase, lo que se hacía, sin cobertura legal expresa, con base en lo dispuesto en el art. 230.1 LOPJ, que, en su redacción actual, dispone que los juzgados y tribunales y las fiscalías están obligados (en la anterior redacción era potestativo) a utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, puestos a su disposición para el desarrollo de su actividad y ejercicio de sus funciones[9].

El uso de la videoconferencia en la Administración de Justicia dio lugar a que el 17 de mayo de 2006 se suscribiese un acuerdo interdepartamental, entre los Ministerios de Justicia e Interior, para la implantación de un sistema de comunicaciones, mediante videoconferencia, entre los centros penitenciarios y las sedes de los Jugados, Tribunales y Ministerio Fiscal, para realizar actuaciones judiciales y comparecencias ante órganos judiciales a través de videoconferencia, de acuerdo con lo dispuesto en los arts. 229.3 LOPJ y 325 LECrim[10].

---

[9] En relación con la regulación del uso de los sistemas de videoconferencia en la Administración de Justicia, la disposición final tercera de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, establecía que el Gobierno debía presentar un proyecto de ley que regulase de manera integral el uso de los sistemas de videoconferencia en la Administración de Justicia, circunstancia que, al menos hasta el momento, no se ha producido.

[10] Vid. la Instrucción 2/2007, de 30 de enero, de la Dirección General de Instituciones Penitenciarias, p. 1.

Sin embargo, ni en la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria (en adelante, LOGP) ni en el Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario (en adelante, RP) se regula el uso de la videoconferencia en el ámbito penitenciario. Tanto una norma como otra parten de que lo normal es que las comunicaciones se realicen de forma oral (presencialmente) y escrita. No obstante, el art. 51.4 LOGP sí prevé expresamente que las comunicaciones previstas en este artículo puedan efectuarse telefónicamente en los casos y con las garantías que se determinen en el RP, lo que nos hace pensar que el legislador concibió las mismas como algo excepcional o novedoso, dado que, en caso contrario, no hubiese hecho mención expresa a esta posibilidad.

Concretamente, las comunicaciones telefónicas se regulan en el art. 47 RP, según el cual, puede autorizarse la comunicación telefónica de los internos, entre otros casos, cuando el interno haya de comunicar algún asunto importante al abogado defensor (art. 47.1.b RP). Para ello, se dice que el interno que desee comunicar telefónicamente con otra persona, debe solicitarlo al Director del establecimiento (art. 47.2 RP), quien, previa comprobación de los mencionados requisitos, autorizará, en su caso, la comunicación y señalará la hora en que deba celebrarse (47.3 RP).

La implantación del sistema de videoconferencia sí se regula en la Instrucción 2/2007, de 30 de enero, de la Dirección General de Instituciones Penitenciarias, que, no obstante, a pesar de que sí regula expresamente el uso de esta tecnología para la celebración de actuaciones judiciales, de comunicaciones con familiares y de consultas médicas[11], no

[11] Vid. http://www.institucionpenitenciaria.es/web/portal/administracionPenitenciaria/TecnologiasInformacion/CalidadServicios.html y http://www.institucionpenitenciaria.es/web/portal//laVidaEnPrision/relacionesExterior/telefono.html (consultados el 1 de julio de 2019). A mayor abundamiento sobre el uso de la videoconferencia para las comunicaciones con familiares y consultas médicas vid. FERNÁNDEZ DÍAZ, Carmen Rocío. Internet Behind Bars: Reality or Utopia? En: OLIVEIRA, Lídia; GRAÇA, Daniela (eds.). *Infocommunication Skills as a Rehabilitation and Social Reintegration Tool for Inmates*. Hershey: IGI Global, 2019. p. 1-23; MARCOS MADRUGA, Florencio de. Las nuevas tecnologías en los centros penitenciarios y sus implicaciones jurídicas. En: MATA Y MARTÍN, Ricardo M. (Dir.); JAVATO MARTÍN, Antonio María (Coord.). *Sistema penitenciario y nuevas tecnologias*. Valladolid:

contempla la posibilidad de hacer uso de la misma para las comunicaciones de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales[12].

2. Antecedentes

Para examinar los antecedentes de las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales, hemos de distinguir entre lo que sucede en la comunidad autónoma de Cataluña, que es la única que tiene trasferidas las competencias en materia penitenciaria, y lo que sucede en el resto de España, donde las competencias sobre instituciones penitenciarias recaen en el Estado y no en las comunidades autónomas[13], por lo que, en principio, todo depende de lo que acuerde la Secretaría General de Instituciones Penitenciarias.

Lex Artis, 2014. p. 239-241; MARTÍN MORAL, María Flora. La utilización del sistema de videoconferencia en el marco de las instituciones penitenciarias. En: MATA Y MARTÍN, Ricardo M. (Dir.); JAVATO MARTÍN, Antonio María (Coord.). *Sistema penitenciario y nuevas tecnologias*. Valladolid: Lex Artis, 2014. p. 45-60; y VIDA FERNÁNDEZ, José. Análisis y propuestas para garantizar el derecho a la asistencia sanitaria de los internos en instituciones penitenciarias. *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, Madrid, n. 62, p. 1-19, 2009.

12 JORDÁN DÍAZ-RONCERO, María José, *Análisis de la implantación*..., cit., pp. 472 y 473, entiende que, aunque de la Instrucción 2/2007, de 30 de enero, de la Dirección General de Instituciones Penitenciarias se extrae que esta comunicación a través de videoconferencia entre abogado e interno no podría mantenerse, dado que ni la LOGP ni el RP lo prohíben, "atendiendo a situaciones adversas que impidan una entrevista que por razones de estrategia procesal relacionadas con el derecho de defensa y de asistencia letrada no puedan ser aplazadas, es obligatorio permitir la reunión por videoconferencia entre abogado e interno en centro penitenciario, pues lo contrario, negar esta petición del letrado o del recluso, implicaría vulneración del derecho de defensa y de la asistencia letrada consagrados ambos en el art. 24.2 CE".

13 En el caso de la comunidad autónoma de Andalucía, a pesar de que, según su Estatuto de Autonomía, corresponde a la comunidad autónoma la competencia ejecutiva en materia penitenciaria (art. 67.3 de la Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía), y pese a que al mes siguiente de la entrada en vigor de este Estatuto se debía designar una Comisión Mixta Paritaria Gobierno-Junta de Andalucía que

Hasta ahora, en España, dos son los antecedentes del uso de la videoconferencia para las comunicaciones entre abogados e internos, precisamente, uno en cada uno de estos ámbitos.

El primero lo encontramos en la comunidad autónoma de Cataluña, donde ya se está implementando un "Servicio de Videoconferencias con centros penitenciarios" para reducir a la mitad las 37.000 visitas presenciales que se hacen cada año entre abogados e internos. Este servicio se puso en marcha tras una prueba piloto que conectó el Centre Penitenciari Quatre Camins (La Roca del Vallés, Barcelona) con el Ilustre Colegio de la Abogacía de Barcelona. Se trata de un servicio que ha puesto en marcha el Ilustre Colegio de la Abogacía de Barcelona conjuntamente con la Dirección General de Servicios Penitenciarios y que garantiza la seguridad y la confidencialidad de esta comunicación[14]. Actualmente, este servicio, pionero en Cataluña y en el resto del Estado, está disponible en nueve centros penitenciarios[15] y tres centros educativos de justicia

---

regulara el proceso, el tiempo y las condiciones de traspaso de las competencias propias de la comunidad autónoma, conforme al presente Estatuto; y que determinara el traspaso de medios personales y materiales necesarios para el ejercicio de tales competencias (número uno de la disposición transitoria primera), lo cierto es que en materia penitenciaria, ningún traspaso de competencia se ha llevado a cabo hasta la fecha. No obstante, recientemente, el 30 de abril de 2019, el Grupo Parlamentario Adelante Andalucía del Parlamento de Andalucía presentó una Proposición no de Ley en Pleno relativa a desarrollo del Estatuto de Autonomía y la competencia de ejecución penitenciaria (Expediente: 11-19/PNLP-000039, número de registro 111913203), disponible en http://www.parlamentodeandalucia.es/webdinamica/portal-web-parlamento/actividadparlamentaria/todaslasiniciativas/porproponente.do?numexp=11-19/PNLP-000039&accion=Ver%20iniciativas&proponente=Grupo%20parlamentario&legislatura=11&indice=510&prop=457 (consultado el 1 de julio de 2019).

[14] Según se dice en la página web del Ilustre Colegio de la Abogacía de Barcelona, "antes de la puesta en funcionamiento del Servicio, se ha llevado a cabo estudio para garantizar la seguridad de la comunicación en forma de videoconferencia. El sistema ha sido revisado y validado por el Centro de Seguridad de la Información de Cataluña". Vid. http://www.icab.es/?go=eaf9d1a0ec5f1dc58757ad6cffdacedb1a58854a600312ccb08705c7052b3548defa77ffbeed6568fa96900438d42b6146cb02bd41ffe8d8 (consultado el 1 de julio de 2019).

[15] Concretamente, en los centros penitenciarios de Quatre Camins (La Roca del Vallés, Barcelona); Brians-1 (San Esteban de Sasroviras, Barcelona); Brians-2 (San Esteban de Sasroviras, Barcelona); Puig de les Basses (Figueras, Gerona);

juvenil[16], con los que se pueden llevar a cabo las videoconferencias desde la sede del Ilustre Colegio de la Abogacía de Barcelona.

Para examinar el segundo antecedente tenemos que remontarnos al año 2017, cuando el Defensor del Pueblo incoó un expediente con la finalidad de conocer si en el ámbito de actuación de la Secretaría General de Instituciones Penitenciarias se había producido alguna iniciativa análoga a la que por aquellas fechas estaba produciéndose en el ámbito de gestión de la Administración penitenciaria de Cataluña: el establecimiento de un sistema de comunicación de letrados con personas privadas de libertad a través de videoconferencia. El Defensor del Pueblo, tras constatar la falta de interés de la Secretaría General de Instituciones Penitenciarias por este asunto, pese a que sí hay, al menos, un aparente interés político en ello[17], recomienda "facilitar las comunicaciones previstas en el artículo 51 de la Ley Orgánica General Penitenciaria entre letrados y personas privadas de libertad, mediante sistemas de videoconferencia, que conecten los colegios de abogados y los centros penitenciarios, de modo que los letrados designados para prestar el servicio de asistencia jurídica gratuita puedan comunicarse con las personas privadas de libertad beneficiarias de este derecho, sin necesidad de desplazarse a los centros penitenciarios"[18].

No obstante, aunque a nivel estatal no hay una iniciativa clara en estas cuestiones, sí ha habido alguna iniciativa particular de algún

---

Lledoners (San Juan de Torruella, Barcelona); Mas d'Enric (El Catllar, Tarragona); Dones (Barcelona, Barcelona); Joves (La Roca del Vallés, Barcelona); Ponent (Lérida, Lérida).

16 Concretamente, en los centros educativos de justicia juvenil de l'Alzina (Palau de Plegamans, Barcelona); Can Llupià (Barcelona, Barcelona) y El Segre (Lérida, Lérida).

17 Vid. el Diario de Sesiones del Congreso de los Diputados, Comisiones, Interior, Sesión n. 39, celebrada el jueves, 13 de diciembre de 2018, n. 691, p. 8, donde se dice que "uno de los objetivos de esta Administración es potenciar la administración digital y las nuevas tecnologías, y en este ámbito, en concreto, para favorecer [...] las videoconferencias entre los internos y sus abogados".

18 Vid. la recomendación del Defensor del Pueblo de 28 de diciembre de 2018 a la Secretaría General de Instituciones Penitenciarias, disponible en https://www.defensordelpueblo.es/resoluciones/comunicacion-entre-los-internos-en-centros-penitenciarios-y-sus-abogados-mediante-videoconferencia/ (consultado el 1 de julio de 2019).

Colegio de Abogados en desarrollar esta cuestión. Concretamente, en febrero de 2019 la Secretaría General de Instituciones Penitenciarias y el Ilustre Colegio de Abogados de Málaga firmaron un convenio experimental, que pretende extenderse al resto de centros de la Administración General del Estado, para que los internos de los centros penitenciarios Málaga I (Alhaurín de la Torre, Málaga) y Málaga II (Archidona, Málaga)[19] puedan comunicarse con sus abogados por videoconferencia.

Así pues, en primer lugar, tras estas primeras experiencias pilotos, habría que implantar este sistema en todo el territorio nacional, para después, a la luz de sus resultados, tratar de replicarla a nivel supranacional, de forma similar a lo que actualmente ya prevé la normativa europea e iberoamericana en otros ámbitos[20].

---

[19] Vid. el Diario de Sesiones del Congreso de los Diputados, Comisiones, Interior, Sesión n. 39, celebrada el jueves, 13 de diciembre de 2018, n. 691, 2018, p. 7, donde, en relación con el sistema de videoconferencia del centro penitenciario de Málaga II (Archidona, Málaga), se dice que "en este momento se está gestionando el correcto funcionamiento del sistema de videoconferencia, ya que este centro podría ser uno de los primeros en España en el que se celebren entrevistas entre los internos y sus abogados a través de videoconferencias".

[20] A mayor abundamiento sobre este tema vid., por ejemplo, el art. 10 del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, hecho en Bruselas el 29 de mayo de 2000; el art. 9 del Segundo Protocolo Adicional al Convenio europeo de asistencia judicial en materia penal, hecho en Estrasburgo el 8 de noviembre de 2001; el Convenio Iberoamericano sobre el uso de la videoconferencia en la Cooperación Internacional entre Sistemas de Justicia, hecho en Mar de Plata el 3 de diciembre de 2010, y su Protocolo adicional relacionado con los costos, régimen jurídico y remisión de solicitudes; o el más reciente art. 24 de la Directiva 2014/41/CE del Parlamento Europeo y del Consejo de 3 de abril de 2014 relativa a la orden europea de investigación en materia penal. Además, sobre este particular es aconsejable consultar JIMENO BULNES, Mar (Coord.). *La cooperación judicial civil y penal en el ámbito de la Unión Europea:* instrumentos procesales. Barcelona: Bosch, 2007; JIMENO BULNES, Mar (Dir.); MIGUEL BARRIO, Rodrigo (Coord.). *Espacio judicial europeo y proceso penal*. Madrid: Tecnos, 2018; y TIRADO ESTRADA, Jesús José. Videoconferencia, cooperación judicial internacional y debido proceso. *Revista de la Secretaría del Tribunal Permanente de Revisión*, Asunción, v. 5, n. 10, p. 153-173, 2017. http://dx.doi.org/10.16890/rstpr.a5.n10.p153

3. Ventajas y desventajas

A nuestro juicio, dos son las principales ventajas de las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales.

En primer lugar, la de que contribuye a garantizar el ejercicio del derecho a la defensa y a la asistencia de letrado cuando el defendido se encuentra interno en un centro penitenciario, facilitando y mejorando la preparación de las actuaciones judiciales que se celebran durante la instrucción y el juicio oral.

En segundo lugar, la de que contribuye a ahorrar tiempo y dinero a los abogados, que tendrán mayores facilidades para trabajar y mayor flexibilidad para concertar reuniones sin depender de desplazamientos (que quedan muy reducidos con el uso de esta tecnología), haciéndolos más compatibles con el resto de su agenda. Esto es especialmente interesante en caso de que al interno, ya lo sea como preso preventivo o como penado, le haya sido reconocido el derecho a la asistencia jurídica gratuita y se le haya nombrado un abogado de oficio. En estos casos, la lejanía de las prisiones de los núcleos de población[21] y la escasa remuneración que estos perciben por su trabajo provoca que, en ocasiones, los abogados desatiendan sus obligaciones y no acudan a los centros penitenciarios a visitar a sus defendidos.

Así pues, las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales serían complementarias, no sustitutivas, de las actualmente previstas en la LOGP y en el RP, es decir, de las comunicaciones orales, presenciales y telefónicas, y escritas[22]. De hecho,

---

[21] MAPELLI CAFFARENA, Borja; BARAS GONZÁLEZ, Marcos. Sistemas de videoconferencia entre abogados y personas privadas de libertad. *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, Madrid, n. 124, p. 3, 2017, hablan muy acertadamente de la "ruralización" en la ubicación de los centros penitenciarios.

[22] Vid. el Acta de la Subcomisión de Derecho Penitenciario del Consejo General de la Abogacía Española (en adelante, CGAE) de 21 de octubre de 2005, p. 4, disponible en http://www.derechopenitenciario.com/comun/fichero.asp?id=2455 (consultado el 1 de julio de 2019), en la que con respecto a la

cada uno de estos medios de comunicación tiene ventajas e inconvenientes según las circunstancias y el momento en el que se empleen. Así, habrá que diferenciar entre la primera o las primeras entrevistas entre el interno y su abogado, en las que la confianza entre ambos puede que aún no se haya fraguado (si no se conocían previamente), y las posteriores, pues en el primer caso las comunicaciones personales parecen más apropiadas a las restantes, incluida la videoconferencia, que se antoja más adecuada cuando

---

entrevista del abogado con su cliente en prisión a través de videoconferencia se dice que, "tras una amplia discusión sobre el particular, la Subcomisión entiende que la entrevista llevada a cabo a través de videoconferencia no debe sustituir a la personal, ya que se perdería perspectiva, sin embargo tampoco se puede renunciar a la utilización de los nuevos medios tecnológicos, por lo que en definitiva entiende que este tipo de entrevista debe ser complementaria a la llevada a cabo personalmente". Sin embargo, en el Acta de la Subcomisión de Derecho Penitenciario del GGAE de 11 de abril de 2014, pp. 4 y 5, disponible en http://www.derechopenitenciario.com/comun/fichero.asp?id=3991 (consultado el 1 de julio de 2019), en relación con el Proyecto Piloto de la Fundación del CGAE e Instituciones Penitenciarias sobre comunicaciones de abogados con sus clientes por videoconferencia, el presidente de la subcomisión, D. Carlos García Castaño, "entiende que es un sistema residual, no complementario, ya que valora la necesidad de ver a los presos y de visitar las prisiones, para fiscalizar, al menos visualmente, la actuación de la Administración Penitenciaria", y, en definitiva, "no le ve mucho futuro". A mayor abundamiento sobre este tema vid. también el Acta de la Subcomisión de Derecho Penitenciario del CGAE de 26 de septiembre de 2014, disponible en http://www.derechopenitenciario.com/comun/fichero.asp?id=3993 (consultado el 1 de julio de 2019). En algunos centros penitenciarios de varios Estados y Condados de Estados Unidos (Arizona-Maricopa; Massachusetts-Bristol; Michigan-Calhoun-Kalamazoo; Texas-Travis; entre otros) ya se han sustituido las comunicaciones presenciales por comunicaciones por videoconferencia. De este modo, con carácter general, los familiares y amigos de los internos no pueden acudir al centro penitenciario a visitarlos, sino solo comunicarse gratuitamente desde unos quioscos con video que funcionan en el centro penitenciario, o descargar una aplicación que les permite hacer videoconferencias desde cualquier teléfono inteligente, con un coste que oscila entre los 8 y los 20 dólares, aproximadamente, para una llamada de unos 20-25 minutos (las comunicaciones con los abogados son gratuitas). Los ingresos obtenidos con este sistema se reparten entre la Administración y el proveedor del servicio. A mayor abundamiento sobre este tema en Texas vid. el documento titulado Video Visitation: how private companies push for visits by video and families pay the price, elaborado por Grassroots Leadership y the Texas Criminal Justice Coalition en octubre de 2014, disponible en http://grassrootsleadership.org/sites/default/files/uploads/Video%20Visitation%20%28web%29.pdf (consultado el 1 de julio de 2019).

la relación entre ambos es más estrecha. Asimismo, habrá que diferenciar entre si el motivo de la comunicación es para cuestiones relevantes, como, por ejemplo, la preparación de la declaración de investigado en la instrucción o el juicio oral, o para cuestiones de trámite, pues, de nuevo, en el primer caso las comunicaciones personales parecen más apropiadas que las restantes, incluida la videoconferencia, que se antoja más adecuada cuando la comunicación tiene por objeto cuestiones de trámite. Del mismo modo, habrá que diferenciar si la comunicación es urgente o no, pues en el primer caso las comunicaciones telefónicas y por videoconferencia parecen más apropiadas a las comunicaciones orales (presenciales) y escritas.

No obstante, las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales también pueden tener una parte negativa, como, por ejemplo, la de que la popularización de este tipo de comunicaciones, dadas las ventajas a las que hemos hecho alusión anteriormente, desplace las comunicaciones orales (presenciales), con la consiguiente pérdida de "contacto físico" entre el interno y su abogado. Otro posible inconveniente del uso de esta tecnología para este fin es la mayor facilidad (al menos, aparentemente) de que este tipo de comunicaciones puedan ser intervenidas u oídas por alguien ajeno a ellas, con el consiguiente aumento de la desconfianza de los intervinientes en la misma (principalmente, del interno) de revelar datos sensibles, pero que pueden ser esenciales para la defensa.

4. Desarrollo

Para ver como podría ser el desarrollo de las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales, en primer lugar, hemos de preguntarnos cuál es la naturaleza de las comunicaciones por videoconferencia, es decir, si estas se han de ajustar a lo dispuesto en relación con las comunicaciones orales (presenciales) o con las comunicaciones telefónicas, ya que según sea una u otra, la regulación de las mismas deberá ser más próxima a lo dispuesto en los arts. 51.1,

2, 3 y 5 LOGP y 42 a 45 y 48 y 49 RP, en el primero de los casos, o en los arts. 51.4 y 47 RP, en el segundo.

A nuestro juicio, la naturaleza de las comunicaciones por videoconferencia es la misma que la de las comunicaciones telefónicas, por lo que hemos de partir de lo dispuesto en los arts. 51.4 LOGP y 47 RP. Sin embargo, como veremos a continuación, las primeras experiencias de comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales no parecen partir de la regulación de este tipo de comunicaciones, sino de lo dispuesto para las comunicaciones orales (presenciales).

4.1. Solicitud

En primer lugar, hemos de preguntarnos cuáles pueden ser las razones que justifiquen el uso de esta tecnología en el ámbito penitenciario. En el ámbito judicial, las razones que justifican el uso de esta tecnología son razones de utilidad, seguridad o de orden público, así como en aquellos supuestos en que la comparecencia de quien haya de intervenir en cualquier tipo de procedimiento penal como investigado o encausado, testigo, perito, o en otra condición resulte particularmente gravosa o perjudicial, y, especialmente, cuando se trate de un menor (arts. 325 y 731 bis LECrim). Sin embargo, en el ámbito penitenciario, las razones que, en nuestra opinión, justifican el uso de esta tecnología son, además de evidentes razones de utilidad, razones de seguridad, de interés del tratamiento y del buen orden del establecimiento (arts. 51.1 LOGP y 41.2 RP). Estas razones constituyen también los límites del uso de la videoconferencia en el ámbito penitenciario, por lo que cabe preguntarse si el uso de esa tecnología para este fin solo debe tener aplicación cuando el interno lo está en un centro penitenciario fuera del ámbito territorial de su abogado, como sostienen algunos[23], o puede tenerlo también con independencia

[23] A mayor abundamiento vid. el Acta de la Subcomisión de Derecho Penitenciario del GGAE de 11 de abril de 2014, pp. 4 y 5, disponible en http://www.derechopenitenciario.com/comun/fichero.asp?id=3991 (consultado el 1 de julio de 2019), en la que, en relación con el Proyecto Piloto de la Fundación del CGAE e Instituciones Penitenciarias sobre comunicaciones de abogados con sus clientes por videoconferencia, el presidente de la subcomisión, D.

de esta circunstancia. En nuestra opinión, el hecho de que el interno se encuentre en un centro penitenciario más o menos cercano al despacho de su abogado no debe ser óbice para que ambos puedan hacer uso de este medio de comunicación.

Por otro lado, hemos de plantearnos quién ha de acordar o quién puede solicitar que las comunicaciones de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales se realicen a través de videoconferencia, si ha de ser el tribunal, de oficio o a instancia de parte; estas últimas por su propia voluntad; o la Administración Penitenciaria. En principio, la intervención judicial no es necesaria salvo supuestos excepcionales, como sucede, por ejemplo, en los supuestos de terrorismo o de internos pertenecientes a bandas o grupos armados, en los que el volante para las comunicaciones orales (presenciales) debe ser expedido por la autoridad judicial que conozca de las correspondientes causas, sin perjuicio de lo dispuesto en el art. 520 LECrim (art. 48.1.2ª RP); ni la de la Administración Penitenciaria, por lo que la solicitud del uso de este sistema queda en manos de los abogados[24].

La solicitud de la comunicación por videoconferencia debe hacerse con una cierta antelación para que los funcionarios puedan llevar al interno al locutorio donde esta se desarrolle y para que puedan organizar las diversas solicitudes de comunicaciones de los internos. No hay un plazo

---

Carlos García Castaño, "entiende que debemos ser restrictivos en su aplicación", por lo que "se plantea por que no solicitar que ambos proyectos, Madrid y Málaga, se hagan para videoconferencias con presos que estén en prisiones fuera de su ámbito territorial, que es lo que tendría más sentido, y no con las prisiones más cercanas como se pretende hacer".

[24] El apartado primero del Conveni de col·laboració entre el Departament de Justícia i el Consell dels Il·lustres Col·legis d'Advocats de Catalunya, per a la implantació del programa de videocomunicacions entre les persones internes en centres penitenciaris i centres educatius de justícia juvenil i els seus advocats defensors, de 23 de març de 2017, p. 3, parece circunscribir el uso de la videoconferencia unicamente a los "que siguin col·legiats dels il·lustres col·legis d'advocats de Catalunya", descartando a los que estén colegiados en otros Colegios de Abogados de España o de otros países. Exactamente lo mismo se prevé en la experiencia piloto puesta en marcha por la Secretaría General de Instituciones Penitenciarias y el Ilustre Colegio de Abogados de Málaga en los centros penitenciarios Málaga I (Alhaurín de la Torre, Málaga) y Málaga II (Archidona, Málaga).

oficial, pero en los proyectos pilotos puestos en marcha actualmente este plazo oscila entre las 48 horas[25] y los cinco días[26].

Actualmente, en relación con las comunicaciones telefónicas, se establece que, salvo casos excepcionales, libremente apreciados por el Director del establecimiento, no se permitirán llamadas desde el exterior a los internos (art. 47.5 RP). En cierto modo, las comunicaciones por videoconferencia podrían ser una excepción a este régimen general cuando fuere el abogado quien llamara por videoconferencia al interno, lo que, no obstante, es totalmente intrascendente en la práctica, ya que, como veremos a continuación, debe haber un concierto previo entre el abogado y el centro penitenciario para que dicha comunicación sea posible.

4.2. Intervinientes

Los intervinientes en las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales pueden ser:

- El interno o los internos, toda vez que el uso de la videoconferencia en los centros penitenciarios como forma de garantizar el ejercicio del derecho a la defensa y a la asistencia de letrado en el proceso penal debe ser posible tanto para las comunicaciones entre internos del mismo o de distintos centros penitenciarios, como para las comunicaciones conjuntas de estos y sus abogados.

---

[25] Vid. el apartado octavo del Conveni de col·laboració entre el Departament de Justícia i el Consell dels Il·lustres Col·legis d'Advocats de Catalunya, per a la implantació del programa de videocomunicacions entre les persones internes en centres penitenciaris i centres educatius de justícia juvenil i els seus advocats defensors, de 23 de març de 2017, p. 6; y MAPELLI CAFFARENA, Borja; BARAS GONZÁLEZ, Marcos. Sistemas de videoconferencia..., cit., p. 4, que estiman "que este plazo, con carácter general, puede ser de 48 horas".

[26] MAPELLI CAFFARENA, Borja; BARAS GONZÁLEZ, Marcos. Sistemas de videoconferencia..., cit., p. 6, nota 4, dicen que en el caso de la experiencia piloto que actualmente se desarrolla en Cataluña "la petición se formula con una antelación mínima de cinco días naturales a la fecha en que quieran comunicarse con su cliente".

Y es que, en efecto, hemos de pensar en la posibilidad del uso de la videoconferencia para las comunicaciones entre internos del mismo o de distintos centros penitenciarios para el ejercicio del derecho de defensa.

Las comunicaciones entre internos del mismo centro penitenciario no aparecen expresamente reguladas ni en la LOGP ni en el RP. En cambio, no ocurre lo mismo con las comunicaciones entre internos de distintos centros penitenciarios, los cuales pueden hacer uso de comunicaciones escritas (art. 46.7ª RP) y telefónicas (art. 47.6 RP). Sin embargo, no se prevé expresamente la posibilidad de comunicaciones orales (presenciales, arts. 42 a 45 RP), aunque quizás ello podría autorizarse si se considerase que los internos que desean comunicar oralmente entre sí son amigos (arts. 51.1 LOGP y 41.1 RP) o allegados (arts. 53 LOGP y 45.1, 3 y 5 RP)[27].

En principio, nada impide que estas comunicaciones entre internos de distintos establecimientos puedan ser entre dos (un interno en cada uno de los centros penitenciarios) o más (uno o varios internos en un centro penitenciario y uno o varios en el otro), e, incluso, porque la tecnología actual así lo permite, entre varios internos situados en tres o más establecimientos. Y es que no hemos de olvidar que las salas de videoconferencia deben tener cabida para un mínimo de cinco internos y un máximo de diez, en función de las disponibilidades de cada uno de los centros[28], por lo que esta circunstancia no es ningún impedimento.

Sin embargo, el primer problema que nos encontramos aquí es que, aunque se prevén las comunicaciones telefónicas entre internos de distintos establecimientos (art. 47.6 RP), estas comunicaciones solo deben autorizarse entre internos que acrediten relación de afectividad o parentesco, lo que excluye, en la mayoría de los casos, que el motivo

---

[27] A mayor abundamiento vid. la Instrucción 4/2005, de 16 de mayo, de la Dirección General de Instituciones Penitenciarias, que, aunque no es especialmente restrictiva con las comunicaciones orales entre internos del mismo centro (p. 7), sí lo es con las de distintos centros (p. 8) cuando señala que "en ningún caso se autorizarán si los Centros están en distinta localidad". Lo mismo sucede con las comunicaciones telefónicas entre internos de distintos centros (p. 9), que "sólo se autorizarán entre internos que acrediten relación de afectividad o parentesco".

[28] Vid. la Instrucción 2/2007, de 30 de enero, de la Dirección General de Instituciones Penitenciarias, p. 2.

de la misma sea el ejercicio del derecho a la defensa y a la asistencia de letrado[29], aunque en algún caso puntual ello sí haya sido autorizado por este motivo[30].

Por tanto, en caso de que la regulación de las comunicaciones por videoconferencia se asimilase en el futuro a la actualmente vigente de las comunicaciones telefónicas, ello impediría el uso de la videoconferencia para las comunicaciones entre internos de distintos establecimientos para el ejercicio de estos derechos.

Además, entendemos que estas, al igual que sucede actualmente con las comunicaciones telefónicas, podrían ser intervenidas mediante resolución motivada del Director en la forma y con los efectos previstos en el art. 46.7ª RP (art. 47.6 RP), por lo que difícilmente pudieran destinarse a este fin ante el temor de los internos de que lo que se dijeran pudiera ser escuchado por personas ajenas a la comunicación.

Otra posibilidad, que actualmente no contempla ni siquiera el RP en relación con las comunicaciones telefónicas, consiste en que esto se desarrolle con la intervención también de los abogados de estos internos o, al menos, de algunos de ellos, con objeto de preparar la defensa, es decir, en el uso de la videoconferencia para las comunicaciones entre internos de distintos establecimientos y sus abogados, estando estos en el centro o los centros penitenciarios o en otros lugares.

Lógicamente, en estos casos, estas comunicaciones no podrían ser intervenidas mediante resolución motivada del Director en la forma y con los efectos previstos en el art. 46.7ª RP, sino que se acogerían al

---

[29] Vid. la Instrucción 4/2005, de 16 de mayo, de la Dirección General de Instituciones Penitenciarias, p. 9.

[30] En efecto, según noticias aparecidas en los medios de comunicación, en relación con líderes del "procés" que se encontraban internos en distintos centros penitenciarios de Cataluña, la dirección del centro penitenciario de Lledoners (San Juan de Torruella, Barcelona), donde estaban internos D. Oriol Junqueras i Vies, D. Raül Romeva i Rueda, D. Jordi Sànchez i Picanyol y D. Jordi Cuixart i Navarro, y del centro penitenciario Puig de les Basses (Figueras, Gerona), donde estaban internas Dña. Dolors Bassa i Coll y Dña. Maria Carme Forcadell i Lluís, autorizó (a nuestro juicio indebidamente, ya que, como estamos viendo, no está previsto su uso para este fin) que estos internos pudieran comunicarse entre ellos por medio de esta vía.

régimen general de la intervención de las comunicaciones de los internos con sus abogados defensores del art. 48.3 RP[31].

- El abogado o los abogados, toda vez que, como acabamos de ver, debería ser posible que en la comunicación por videoconferencia pudieran estar presente el abogado o los abogados del interno o de los internos y el abogado o los abogados de otro u otros internos por la misma causa. Asimismo, también debería ser posible que estuvieran presentes estudiantes de Grado o Máster que fuesen becarios o pasantes de alguno de estos abogados.

- El funcionario o los funcionarios, toda vez que la celebración de cualquier videoconferencia debe estar controlada por uno o varios funcionarios, en función del número y características de los internos desplazados. Si bien estos, por razones de confidencialidad no pueden intervenir directamente en la comunicación, como veremos a continuación, el funcionario o los funcionarios deberán comprobar no solo la identidad del interno, sino también la del abogado[32] y, en su caso, la de otros intervinientes.

- Otros intervinientes. Actualmente, mientras que en la experiencia piloto puesta en marcha por la Secretaría General de Instituciones Penitenciarias y el Ilustre Colegio de Abogados de Málaga se prevé que en las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales no puedan participar terceras personas, salvo que sea estrictamente necesario (como un intérprete), ya que, según se dice, este tipo de comunicaciones están sujetas al mismo reglamento que rige las entrevistas personales, algunos autores sostienen que el abogado también ha de poder estar acompañado por las personas que este, en su

---

[31] A mayor abundamiento sobre este tema vid. los arts. 118.4 LECrim y 51.2 LOGP; y RODRÍGUEZ ÁLVAREZ, Ana; GARCÍA MONTEAGUDO, Alexandre. La intervención de las comunicaciones telefónicas y telemáticas entre el abogado y el investigado. En: BUENO DE MATA, Federico (Dir./Coord.). *FODERTICS 6.0: los nuevos retos del derecho ante la era digital*. Granada: Comares, 2017. p. 183-194.

[32] Aunque, como veremos más adelante, en las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales esto también puede corresponderle al Colegio de Abogados con respecto a sus colegiados.

caso, autorizare[33]. Como ya hemos dicho anteriormente, parece lógico que el abogado pudiera estar acompañado por otro abogado, de su despacho o no, por un pasante, por un intérprete, o por un perito. En cambio, no parece que deba ser posible que otras personas ajenas a la defensa, como, por ejemplo, familiares del interno, deban poder estar presentes, de forma que la comunicación por videoconferencia con el abogado se utilizara indebidamente para hacer otro tipo de comunicación. Bien es cierto que, en la actualidad, esto es perfectamente posible que suceda en las comunicaciones telefónicas con el abogado, pues no hay ningún sistema que garantice que en el despacho del abogado o donde este se encuentre no esté, junto a él, un familiar del interno o cualquier otra persona que hable con él. A pesar de ello, entendemos que al tiempo de la solicitud de cita de la comunicación por videoconferencia con el abogado, lo que, a nuestro juicio, dicho sea de paso, debería hacerse por medio de las nuevas tecnologías (app, página web, o similar), este debería especificar si a la videoconferencia acudirá solo o acompañado, y, en este caso, por quién, especificando sus datos personales y el motivo de su presencia, de forma que esto se tenga en cuenta a la hora de autorizar o no la comunicación y pueda ser controlado posteriormente, el día en que se lleve a cabo la misma, por el funcionario o los funcionarios.

4.3. Identificación de los intervinientes

Con respecto a la identificación de los intervinientes, habrá que distinguir entre la identificación de los internos y la de los abogados y, en su caso, terceras personas.

La identificación de los internos se hará a través del Documento de Identificación Interior, cacheo de los mismos y revisión con la raqueta o arco detector, debiendo verificarse previamente, además, la existencia de posibles incompatibilidades entre los internos participantes, si fueran varios[34].

---

[33] Vid. MAPELLI CAFFARENA, Borja; BARAS GONZÁLEZ, Marcos. Sistemas de videoconferencia..., cit, p. 4.

[34] Vid. la Instrucción 2/2007, de 30 de enero, de la Dirección General de Instituciones Penitenciarias, p. 6.

Durante la celebración de la videoconferencia los internos deben poder portar aquellos objetos necesarios para el buen fin de la comunicación con sus abogados y deben poder exhibir documentos u objetos sin que sea necesario que por razones debidamente justificadas la Dirección del centro lo haya autorizado[35]. Es decir, la regla general ha de ser que los internos puedan portar y exhibir estos documentos u objetos, salvo que por razones debidamente justificadas[36] la Dirección del centro lo haya denegado.

Por otro lado, para la celebración de las comunicaciones de los internos con sus abogados defensores se debe identificar al comunicante mediante la presentación del documento oficial que le acredite como abogado en ejercicio (art. 48.1.1ª RP), es decir, mediante su carné de colegiado en el colegio de abogados de que se trate, que se le podrá requerir por el funcionario de Instituciones Penitenciarias encargado de la videoconferencia.

Además, el comunicante habrá de presentar un volante de su respectivo Colegio, en el que conste expresamente su condición de defensor del interno en las causas que se siguieran contra el mismo o como consecuencia de las cuales estuviera cumpliendo condena. En los supuestos de terrorismo o de internos pertenecientes a bandas o grupos armados, como ya hemos dicho anteriormente, el volante deberá ser expedido por la autoridad judicial que conozca de las correspondientes causas, sin perjuicio de lo dispuesto en el art. 520 LECrim (art. 48.1.2ª RP).

A diferencia de lo que se prevé para los internos (cacheo de los mismos y revisión con la raqueta o arco detector) y para los abogados en las comunicaciones orales (presenciales), en las comunicaciones por videoconferencia esto carece de sentido para estos últimos, toda vez que los mismos se encuentran en todo momento fuera del centro penitenciario. No obstante, en la experiencia piloto puesta en marcha por la Secretaría General de Instituciones Penitenciarias y el Ilustre Colegio de Abogados

---

[35] Al contrario de lo que actualmente dispone la Instrucción 2/2007, de 30 de enero, de la Dirección General de Instituciones Penitenciarias, p. 6.

[36] Como, por ejemplo, razones de seguridad, de interés del tratamiento y del buen orden del establecimiento (arts. 51.1 LOGP y 41.2 RP).

de Málaga se prevé que los abogados deban demostrar que no van a utilizar dispositivos que permitan la grabación[37] o la llamada de otras personas durante las sesiones de videoconferencias[38], es decir, que el abogado no podrá llevar su teléfono móvil o cualquier otro dispositivo tecnológico que le permita comunicarse con terceras personas, lo que plantea la duda de cómo habrá de llevarse esto a cabo, teniendo en cuenta que el abogado, al estar fuera del centro penitenciario (en las dependencias del Colegio de Abogados o en otro sitio), no puede ser sometido a revisión con raqueta o arco detector ni cacheado por los funcionarios, como sí sucede en las comunicaciones orales (presenciales).

Así pues, la identificación de los abogados puede ser doble: virtual, por los funcionarios de prisiones desde el centro penitenciario a través del sistema de videoconferencia, y presencial, por los trabajadores del Colegio de Abogados en el lugar desde donde esta se desarrolle[39], que normalmente, como veremos a continuación, será el Colegio de Abogados.

---

[37] MAPELLI CAFFARENA, Borja; BARAS GONZÁLEZ, Marcos. Sistemas de videoconferencia..., cit., p. 3, parecen dejar abierta la puerta a que las conversaciones por videoconferencia puedan ser grabadas cuando dicen que con ellas se pretende "facilitar en determinadas circunstancias la incorporación a un soporte informático de las entrevistas con su cliente con el objetivo de que el Abogado pueda hacer uso del mismo en el desarrollo de la defensa —presentarlo como prueba, transferirlo a otros colegas, archivo, etc. —".

[38] Como ya hemos dicho anteriormente, esto es perfectamente posible que suceda en las comunicaciones telefónicas con el abogado, pues no hay ningún sistema que garantice que estos no están grabando la llamada o que en el despacho del abogado o donde este se encuentre no esté, junto a él, un familiar del interno o cualquier otra persona que hable con él.

[39] Por esta segunda opción es por la que se ha optado en la experiencia piloto que actualmente se desarrolla en Cataluña, donde el apartado noveno del Conveni de col·laboració entre el Departament de Justícia i el Consell dels Il·lustres Col·legis d'Advocats de Catalunya, per a la implantació del programa de videocomunicacions entre les persones internes en centres penitenciaris i centres educatius de justícia juvenil i els seus advocats defensors, de 23 de març de 2017, p. 7, dice que "arribat el moment en què s'hagi d'establir la comunicació, l'il·lustre col·legi haurà de confirmar que la persona que es presenta com a advocat és efectivament la persona designada en el moment de fer la petició i no permetrà que se celebri si es presenta una altra persona en el seu lloc".

4.4. Lugar

Con respecto al lugar de las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales hemos de advertir que realmente hemos de hablar más bien de lugares, ya que estas se desarrollan al mismo tiempo desde dos o más sitios distintos. Así pues, hemos de distinguir entre el lugar donde se encuentre el interno, que, en todo caso, será dentro del centro penitenciario, y el lugar donde se encuentre el abogado, que, en todo caso, será fuera del centro penitenciario, toda vez que, en caso contrario, no tendría sentido hacer uso de este medio de comunicación.

En cuanto al lugar donde se encuentre el interno, estas comunicaciones deben celebrarse en locutorios especiales, en los que quede asegurado que el control del funcionario encargado del servicio sea solamente visual (arts. 47.4 y 48.1.3ª RP).

Aunque las salas de videoconferencias deben disponer, además de la zona para internos, de una zona contigua, para la estancia de funcionarios, separadas, ambas, por una mampara de visión unidireccional, para el adecuado control visual[40], el problema es que de esta forma realmente pueda garantizarse la confidencialidad de las comunicaciones entre el interno y su abogado.

Por ello, aunque se prevé[41] que su uso solo se dé cuando no sea posible la instalación de mampara de cristal de visión unidireccional, a nuestro juicio, sería más conveniente que el control visual se hiciera, en su caso, mediante una cámara de seguridad que careciese de micrófonos que le permitiesen captar el sonido, lo que permitiría alejar a los funcionarios del lugar donde se estuviese desarrollando la comunicación, y, con ello, se despejaría el posible temor de los comunicantes de que la comunicación estuviese siendo oída por los funcionarios[42]. Lógicamente, este sistema

---

[40] Vid. la Instrucción 2/2007, de 30 de enero, de la Dirección General de Instituciones Penitenciarias, p. 3.

[41] Ibídem, pp. 3 y 5, donde se dice que "el control se realizará desde la cabina de seguridad y a través de la mampara de cristal unidireccional o, en su defecto, por circuito cerrado de TV".

[42] Tal como actualmente se prevé en el apartado sexto del Conveni de col·laboració entre el Departament de Justícia i el Consell dels Il·lustres Col·legis

debería implicar a su vez dos cosas: la primera es que la cámara de seguridad debería estar situada de tal forma que impidiese que se pudiera leer los labios de los comunicantes y los documentos de que pudieran hacer uso, y, en segundo lugar, que en el locutorio debería haber un cartel informativo en el que se advirtiese de que no se graba el vídeo ni se almacena lo grabado, sino que el sistema de videovigilancia solo permite la visión en directo de la imagen, pero no del audio.

La sala de la videoconferencia también debe estar dotada de un sistema de intercomunicación entre la sala y la cabina de seguridad, aunque dicho sistema debe impedir que el funcionario pueda oír lo que en ella se dice.

El funcionario podrá entrar con el interno en el locutorio donde se halle el equipo de videoconferencia para activar el mismo y comprobar que la comunicación es posible, pero deberá ausentarse antes de que verdaderamente comience la comunicación entre el interno y su abogado para respetar la confidencialidad de la misma. No obstante, deberá controlar visualmente su desarrollo. Actualmente, esto plantea el problema del aislamiento acústico de los locutorios en los que se desarrollan la videoconferencia. Estos no suelen ser habitáculos totalmente aislados acústicamente, lo que permite que, en ocasiones, quien está fuera pueda oír lo que se dice en su interior. Hemos de tener en cuenta que el sistema actual de videoconferencia, en muchos casos, hace que lo que el interno oye o lo que dice esté a un volumen muy elevado, por lo que puede filtrarse al exterior. Este no es un tema baladí, como pudiera parecer, sino que, muy al contrario, puede suponer una merma real al efectivo ejercicio del derecho a la defensa[43].

---

d'Advocats de Catalunya, per a la implantació del programa de videocomunicacions entre les persones internes en centres penitenciaris i centres educatius de justícia juvenil i els seus advocats defensors, de 23 de març de 2017, p. 5, que, al respecto dice que "per tal de garantir en tot moment la confidencialitat de les comunicacions advocat-persona interna, aquests locutoris disposaran d'un sistema de videovigilància amb senyal únicament visual".

[43] A mayor abundamiento vid. la Sentencia del Tribunal Europeo de Derechos Humanos de 13 de mayo de 2007 (caso Castravet contra Moldavia), según la cual, aplicando analógicamente lo que señalaba la defensa del Sr. Castravet con respecto al uso de la mampara en los locutorios al ámbito que ahora nos ocupa, la videoconferencia crea una barrera para la confidencialidad, ya que

En cuanto al lugar donde se encuentre el abogado, este puede ser el despacho del abogado o cualquier otro sitio donde este se encuentre, el Colegio de Abogados, un juzgado o tribunal u otras dependencias públicas o privadas.

MAPELLI CAFFARENA y BARAS GONZÁLEZ[44] entienden que "en un primer momento y hasta la consolidación del sistema las videoconferencias se realizarán desde las sedes de los Colegios de Abogados, pero una vez consolidado el procedimiento, [...], se podrá realizar directamente desde los despachos profesionales o, incluso desde un dispositivo móvil del Abogado siempre cumpliendo las garantías de privacidad y protección de datos necesarias". Y es que, en efecto, los dispositivos tecnológicos actuales permiten, al igual que sucede con las comunicaciones telefónicas, que los abogados puedan comunicarse por videoconferencia desde cualquier lugar mediante su teléfono móvil o su ordenador.

Sin embargo, en la experiencia piloto puesta en marcha por la Secretaría General de Instituciones Penitenciarias y el Ilustre Colegio de Abogados de Málaga se prevé que los abogados solo pueden comunicarse con sus clientes a través de unos puestos específicos ubicados en la sede del Colegio o en una de sus nueve delegaciones, nunca desde un dispositivo propio o desde el despacho del abogado, un juzgado o tribunal u otras dependencias públicas o privadas.

A nuestro juicio, no debería haber inconveniente en que estas comunicaciones se celebrasen desde cualquiera de estos lugares, especialmente desde el despacho del abogado, desde el que, como ya hemos dicho anteriormente, ya es posible mantener comunicaciones telefónicas incluso, hipotéticamente, con una o varias personas (a través del sistema

---

tanto el preso como su abogado deben alzar la voz para poder oírse, gritos que habrían facilitado la intercepción o grabación de su conversación y que, en cualquier caso, sus gritos generaban el riesgo de que su discusión fuese escuchada por los guardas o a través de la puerta. Este riesgo de escucha es suficiente, pues, como ha dicho el Tribunal Europeo de Derechos Humanos en esta sentencia, "tal creencia inhibiría inevitablemente la libertad de discusión entre el abogado y el cliente".

44 Vid. MAPELLI CAFFARENA, Borja; BARAS GONZÁLEZ, Marcos. Sistemas de videoconferencia..., cit., p. 4.

de manos libres) ajenas al despacho. Pudiera pensarse que el motivo de que ello no se permita se debe a razones de seguridad, ante la posibilidad de que las comunicaciones efectuadas desde estos lugares puedan hacerse a través de canales poco seguros que permitan su interceptación o ante el temor de que se usen para comunicarse con familiares y otras personas, pero, como venimos diciendo, ambos riesgos están también presentes en las comunicaciones telefónicas, que, sin embargo, están plenamente admitidas y no generan esta desconfianza.

4.5. Tiempo

También hemos de analizar el tiempo (periocidad y duración) en el que dicha comunicación por videoconferencia es posible.

La periodicidad y duración de las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales dependerá, entre otras cuestiones, de los recursos materiales[45] y humanos disponibles y del número de solicitudes de abogados e internos que quieran hacer uso de este medio de comunicación.

En el caso de las comunicaciones orales (presenciales) con abogados, respecto al tiempo de la visita, hemos de decir que las mismas, a diferencia de lo que sucede con las que se llevan a cabo con sus familiares, amigos y representantes acreditados de organismos e instituciones de cooperación penitenciaria, no están sujetas a plazo.

Sin embargo, en el caso de las comunicaciones telefónicas, estas, siempre que las circunstancias del establecimiento lo permitan, deben efectuarse con una frecuencia máxima de cinco llamadas por semana y no deben tener una duración superior a cinco minutos (art. 47.4 RP)[46],

[45] Así, por ejemplo, en el Centre Penitenciari Brians 1 (San Esteban de Sasroviras, Barcelona) se han instalado ocho equipos con capacidad para 16.000 comunicaciones anuales.

[46] Aunque actualmente, con carácter general, se permiten hasta diez llamadas por semana de hasta ocho minutos cada una, al igual que ya sucedía en los centros penitenciarios de la comunidad autónoma de Cataluña.

límite dentro del cual deben entenderse incluidas las comunicaciones con el abogado[47].

Por ello cabe preguntarse cuál debe ser la duración de las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales. Si lo que se quiere es evitar desplazamientos al centro penitenciario, no parece lógico que, en este caso, la comunicación pueda tener una duración tan restringida como la que actualmente tienen las comunicaciones telefónicas, siendo más adecuado, a nuestro juicio, que esta comunicación se acerque, lo más posible, a la duración "sin límites" que tienen actualmente las comunicaciones orales (presenciales). Con carácter ordinario, se podría fijar una duración de 30 minutos[48], con

---

47 Vid. el razonamiento jurídico segundo del Auto del Juzgado Central de Vigilancia Penitenciaria de 6 de junio de 2014. En el mismo sentido se pronuncia el Auto del Juzgado de Vigilancia Penitenciaria de Ciudad Real de 15 de abril de 2002, donde se analiza un supuesto en el que "el interno formula queja contra la decisión del Centro por contabilizar la llamada telefónica del interno a su abogado dentro de las dos llamadas semanales a su familia". En efecto, "en el Centro se autorizan solo dos llamadas telefónicas semanales, incluidas las del abogado, ya que no excepciona éstas del resto de llamadas", y se recuerda que el art. 47 RP "no excepciona las llamadas telefónicas con los abogados del resto de las llamadas, por lo que el límite, genérico de cinco llamadas telefónicas, debe entenderse del total de llamadas telefónicas". Esta misma línea se sigue en el Auto de la Audiencia Provincial de Ciudad Real de 2 de junio de 2003, según el cual, "los internos [...] tendrán derecho a comunicar telefónicamente con sus familiares cinco veces a la semana en los términos del artículo 47.4 del Reglamento Penitenciario, de cuyo cupo máximo se deducirán, en su caso, las llamadas telefónicas que el interno realice a su abogado defensor o a otras personas". No obstante, "el Gobierno va a llevar a cabo una modificación en la aplicación informática para que el sistema no contabilice las llamadas del interno al abogado en el cupo de llamadas autorizadas", tal como consta en la respuesta del Gobierno de 11 de julio de 2018 a la pregunta escrita que el senador D. Jon Iñarritu García, Senador del Euskal Herria Bildu (EH Bildu) designado por el Parlamento Vasco, del Grupo Parlamentario Mixto (GPMX), formuló al Gobierno sobre este particular el 3 de mayo de 2018. A mayor abundamiento vid. http://www.senado.es/web/actividadparlamentaria/iniciativas/detalleiniciativa/textosexpedientes/index.html?legis=12&id1=684&id2=044687 (consultado el 1 de julio de 2019).

48 Aunque MAPELLI CAFFARENA, Borja; BARAS GONZÁLEZ, Marcos. Sistemas de videoconferencia..., cit., p. 6, nota 4, dicen que en la experiencia piloto que actualmente se desarrolla en Cataluña, los tramos horarios son "de media hora para cada visita", como consta en el apartado séptimo del

independencia de que, según la demanda, esta pudiera prolongarse como si de una comunicación oral (presencial) se tratase.

Del mismo modo, en la experiencia piloto puesta en marcha por la Secretaría General de Instituciones Penitenciarias y el Ilustre Colegio de Abogados de Málaga únicamente se prevé que las entrevistas con los abogados puedan celebrarse, de momento, de lunes a jueves, en horario de 17:30 a 19:30 h. y con un intervalo de quince minutos que permita el relevo de internos en la sala de videoconferencia. El hecho de que las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales solo sean por las tardes y en un horario concreto restringe lo dispuesto en el régimen de comunicaciones orales (presenciales, no en el caso de las telefónicas, como hemos visto), y, aunque el tiempo de la visita tan solo se puede restringir por razones de seguridad, de interés del tratamiento y del buen orden del establecimiento (arts. 51.1 LOGP y 41.2 RP), entendemos que ello está justificado, al menos en estos momentos iniciales en los que de lo que se trata es de poner en marcha el sistema[49]. Aún así, uno de los aspectos negativos de que la comunicación

Conveni de col·laboració entre el Departament de Justícia i el Consell dels Il·lustres Col·legis d'Advocats de Catalunya, per a la implantació del programa de videocomunicacions entre les persones internes en centres penitenciaris i centres educatius de justícia juvenil i els seus advocats defensors, de 23 de març de 2017, pp. 5 y 6, "la durada màxima de les videocomunicacions serà de 60 minuts, amb caràcter general. En el moment de fer la reserva a l'agenda, el col·legi haurà de concretar quina serà la durada de la comunicació (10, 15, 20, 30 minuts, etc., fins a un màxim de 60 amb caràcter general). Si per causes degudament justificades es considera que la videoconferència ha de durar més d'aquest temps, en el moment de fer la reserva a l'agenda corresponent es podrà reservar per un temps superior, tot ajustant-se a les necessitats reals i amb l'objectiu de fer un ús eficient dels espais". A mayor abundamiento vid. también la Resolució JUS/524/2018, de 19 de març, per la qual es determinen els horaris d'admissions voluntàries en els centres penitenciaris de Catalunya i de comunicacions presencials de les persones internes amb advocats i altres professionals.

[49] Esto es lo que sucedió en la experiencia piloto que actualmente se desarrolla en Cataluña, tal como consta en el apartado séptimo del Conveni de col·laboració entre el Departament de Justícia i el Consell dels Il·lustres Col·legis d'Advocats de Catalunya, per a la implantació del programa de videocomunicacions entre les persones internes en centres penitenciaris i centres educatius de justícia juvenil i els seus advocats defensors, de 23 de març de 2017,

por videoconferencia solo pueda hacerse desde el Colegio de Abogados y no desde el despacho del abogado o desde cualquier otro lugar en el que este se encuentre es que estas siempre dependerán del horario de aquel, además del que imponga el centro penitenciario.

Para concluir, no hemos de olvidar que, aunque estas comunicaciones, al igual que sucede actualmente con las orales (presenciales), deben registrarse por orden cronológico en el libro correspondiente, consignándose el nombre y apellidos de los comunicantes del interno, el número de la causa y el tiempo de duración de la visita (art. 48.1.3ª RP)[50], esta constancia no puede suponer quebrar la confidencialidad de las mismas, por lo que estas no podrán ser oídas ni grabadas por la Administración Penitenciaria, más allá de en los casos en los que ello se permite legalmente.

4.6. Otras cuestiones

Finalmente, conviene examinar otras cuestiones que pueden tener una gran trascendencia en el desarrollo de las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales.

Así, en primer lugar, cabe preguntarse qué sucede en caso de que los equipos de videoconferencia instalados en el centro penitenciario no sean suficientes para atender la demanda. En este sentido, no hemos de olvidar que, como ya hemos dicho anteriormente, el uso de estos equipos trasciende el objeto de este trabajo, extendiéndose también a otros ámbitos como, por ejemplo, la celebración de actuaciones

---

p. 5, cuando dice que "prèviament a l'entrada en funcionament de l'agenda digital, l'horari de funcionament dels videolocutoris serà únicament de matí, de 9.15 h a 13.15 hores, de dilluns a divendres no festius. L'entrada en funcionament de l'agenda digital possibilitarà també un horari de tarda, de 15.30 a 19.30 hores".

[50] Al respecto vid. el apartado undécimo del Conveni de col·laboració entre el Departament de Justícia i el Consell dels Il·lustres Col·legis d'Advocats de Catalunya, per a la implantació del programa de videocomunicacions entre les persones internes en centres penitenciaris i centres educatius de justícia juvenil i els seus advocats defensors, de 23 de març de 2017, pp. 7 y 8.

judiciales, comunicaciones entre internos y familiares y consultas médicas. Lógicamente, este problema será más frecuente que surja cuanto mayor sea la demanda del sistema y menos equipos existan, por lo que los recursos materiales juegan aquí un papel trascendental. No obstante, entendemos que, a falta de equipos suficientes, debe tener preferencia, por este orden, la celebración de consultas médicas urgentes (lo que no parece lo más probable que suceda en la práctica), la celebración de actuaciones judiciales, las comunicaciones de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales, y, en último lugar, las comunicaciones entre internos y familiares[51].

También hemos de plantearnos quién ha de sufragar el uso de esta tecnología. En este sentido, ha de tenerse en cuenta que, en relación con las comunicaciones telefónicas, se establece que el importe de la llamada será satisfecho por el interno, salvo cuando se trate de la comunicación prevista en el art. 41.3 RP, es decir, salvo la llamada para que el interno pueda comunicar inmediatamente a su familia y abogado su ingreso en un centro penitenciario, así como su traslado a otro establecimiento en el momento del ingreso (art. 47.4 RP). En el caso de las comunicaciones por videoconferencia, al menos hasta ahora, su coste está siendo sufragado por la Administración Pública o por los Colegios de Abogados[52], pero no

---

[51] En contra se pronuncia el apartado décimo del Conveni de col·laboració entre el Departament de Justícia i el Consell dels Il·lustres Col·legis d'Advocats de Catalunya, per a la implantació del programa de videocomunicacions entre les persones internes en centres penitenciaris i centres educatius de justícia juvenil i els seus advocats defensors, de 23 de març de 2017, p. 7, que da prioridad a las comunicaciones entre internos y familiares frente a las de los internos con sus abogados cuando dice que "cada centre penitenciari disposarà de tres espais de VCO: un es destinarà a les comunicacions judicials (sala de VCO), un altre a les VCO amb advocats (locutori 1) i l'altre a les comunicacions amb familiars (locutori 2). En cas que calgui, i sempre que estigui lliure, el locutori 2 es podrà utilitzar per a comunicacions judicials i amb lletrats. En el cas que els dos locutoris i la sala estiguin ocupats per agenda i es produeixi una urgència judicial, aquesta s'haurà d'acomodar dins del locutori 1, de manera que es preservin sempre les comunicacions familiars previstes".

[52] Según consta en el Acta de la Subcomisión de Derecho Penitenciario del GGAE de 11 de abril de 2014, pp. 4 y 5, disponible en http://www.derechopenitenciario.com/comun/fichero.asp?id=3991 (consultado el 1 de julio de 2019), el coste de estos proyectos pilotos corre, al menos por ahora, "a costa de los colegios de abogados [...] ya que la Administración no va a pagar

es descabellado pensar que en un futuro próximo, en la medida que pueda extenderse este servicio, el mismo deje de ser gratuito para el interno o para su abogado[53]. Por ello, a nuestro juicio, se debería contemplar expresamente algo parecido a lo que actualmente dispone el art. 123.1 LECrim en relación con el derecho a la traducción e interpretación, de forma que los gastos de la videoconferencia sean sufragados por la Administración.

Por otro lado, hemos de advertir que el sistema actual no prevé la posibilidad de que el abogado pueda mostrar documentos a su defendido por vía telemática, por lo que en estos casos, deberá desplazarse personalmente hasta el centro penitenciario con los documentos impresos o, muy excepcionalmente, en formato electrónico, posibilidad esta última que actualmente también se está experimentado en algunos centros penitenciarios de nuestro país como proyecto piloto.

Conclusiones

Las comunicaciones por videoconferencia, en general, y las de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales, en particular, deberían regularse en la LOGP y/o en el RP, que actualmente son ajenos a la existencia de este medio de comunicación, además de desarrollarse en las Instrucciones que desde ese momento en adelante dictase la Secretaría General de Instituciones Penitenciarias.

Estas comunicaciones deben ser complementarias, no sustitutivas, de las actualmente previstas en la LOGP y en el RP, es decir, de las comunicaciones orales, presenciales y telefónicas, y escritas, y, en el caso de las de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales, constituyen una

---

ni un duro. (Instituciones Penitenciario [sic.] y la Fundación del CGAE) [...] y la experiencia piloto tendrá lugar en mayo o junio con un coste de 9.000 euros por Colegio".

53 Así sucede en otros países de nuestro entorno, como, por ejemplo, en Estados Unidos.

forma de garantizar el ejercicio del derecho a la defensa y a la asistencia de letrado en el proceso penal, por lo que deben tener la protección que establece el art. 48.3 RP.

Precisamente por este motivo es necesario adoptar medidas como las que se proponen en este trabajo para el desarrollo de las mismas, de forma que su solicitud sea tremendamente ágil y sencilla, el abogado pueda intervenir en la videoconferencia desde su despacho o cualquier otro lugar donde se encuentre, y exista un número adecuado de recursos materiales y humanos que permitan que la periocidad y duración de este tipo de comunicaciones no sea vea lastrada por la falta de equipos o funcionarios. Del mismo modo, la gratuidad del sistema para el interno y su abogado, así como la posibilidad de que este pudiera mostrar documentos a su defendido por vía telemática, contribuirían enormemente al uso de la videoconferencia en las comunicaciones de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales.

Bibliografía

FERNÁNDEZ DÍAZ, Carmen Rocío. Internet Behind Bars: Reality or Utopia? En: OLIVEIRA, Lídia; GRAÇA, Daniela (eds.). *Infocommunication Skills as a Rehabilitation and Social Reintegration Tool for Inmates*. Hershey: IGI Global, 2019. p. 1-23.

GUTIÉRREZ BARRENENGOA, Ainhoa. La utilización de la videoconferencia en la Administración de Justicia. En: HERRÁN ORTIZ, Ana Isabel; EMALDI CIRIÓN, Aitziber; ENCISO SANTOCILDES, Marta (Eds.), *Derecho y Nuevas Tecnologías*. Bilbao: Universidad de Deusto, 2010. v. 2, p. 121-134.

JIMENO BULNES, Mar (Coord.). *La cooperación judicial civil y penal en el ámbito de la Unión Europea:* instrumentos procesales. Barcelona: Bosch, 2007.

JIMENO BULNES, Mar (Dir.); MIGUEL BARRIO, Rodrigo (Coord.). *Espacio judicial europeo y proceso penal*. Madrid: Tecnos, 2018.

JORDÁN DÍAZ-RONCERO, María José. *Análisis de la implantación y eficacia de la videoconferencia en el proceso penal español: hacia una modernización de nuestro sistema de justicia penal*. Tesis Doctoral (Programa de Doctorado en Derecho,

Empresa y Justicia) – Universidad de Valencia, Valencia, 2014. Disponible en: <http://roderic.uv.es/handle/10550/44107>. Consultado el: 1 jul. 2019.

MARCOS MADRUGA, Florencio de. Las nuevas tecnologías en los centros penitenciarios y sus implicaciones jurídicas. En: MATA Y MARTÍN, Ricardo M. (Dir.); JAVATO MARTÍN, Antonio María (Coord.). *Sistema penitenciario y nuevas tecnologias*. Valladolid: Lex Artis, 2014. p. 225-249.

MAPELLI CAFFARENA, Borja; BARAS GONZÁLEZ, Marcos. Sistemas de videoconferencia entre abogados y personas privadas de libertad. *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, Madrid, n. 124, p. 1-7, 2017.

MARTÍN MORAL, María Flora. La utilización del sistema de videoconferencia en el marco de las instituciones penitenciarias. En: MATA Y MARTÍN, Ricardo M. (Dir.); JAVATO MARTÍN, Antonio María (Coord.). *Sistema penitenciario y nuevas tecnologias*. Valladolid: Lex Artis, 2014. p. 45-60.

RODRÍGUEZ ÁLVAREZ, Ana; GARCÍA MONTEAGUDO, Alexandre. La intervención de las comunicaciones telefónicas y telemáticas entre el abogado y el investigado. En: BUENO DE MATA, Federico (Dir./Coord.). *FODERTICS 6.0: los nuevos retos del derecho ante la era digital*. Granada: Comares, 2017. p. 183-194.

TIRADO ESTRADA, Jesús José. Videoconferencia, cooperación judicial internacional y debido proceso. *Revista de la Secretaría del Tribunal Permanente de Revisión*, Asunción, v. 5, n. 10, p. 153-173, 2017. http://dx.doi.org/10.16890/rstpr.a5.n10.p153

VALBUENA GONZÁLEZ, Félix. Proceso penal y videoconferencia. En: HERRÁN ORTIZ, Ana Isabel; EMALDI CIRIÓN, Aitziber; ENCISO SANTOCILDES, Marta (Eds.), *Derecho y Nuevas Tecnologías*. Bilbao: Universidad de Deusto, 2010. v. 3, p. 83-95.

VIDA FERNÁNDEZ, José. Análisis y propuestas para garantizar el derecho a la asistencia sanitaria de los internos en instituciones penitenciarias. *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, Madrid, n. 62, p. 1-19, 2009.

Informações adicionais e declarações dos autores
(integridade científica)

Declaração de conflito de interesses (conflict of interest declaration): o autor confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

Declaração de ineditismo e originalidade (declaration of originality): o autor assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 09/07/2019
- Controle preliminar e verificação de plágio: 12/07/2019
- Avaliação 1: 24/07/2019
- Avaliação 2: 25/07/2019
- Avaliação 3: 27/07/2019
- Decisão editorial preliminar: 27/08/2019
- Retorno rodada de correções: 10/09/2019
- Decisão editorial final: 24/09/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editora-associada: 1 (CC)
- Revisores: 3

COMO CITAR ESTE ARTIGO:

GARCÍA MOLINA, Pablo. Las comunicaciones por videoconferencia de los internos con el abogado defensor o con el abogado expresamente llamado en relación con asuntos penales. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 5, n. 3, p. 1219-1254, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.255

Nuove tecnologie e compressione della libertà personale: la sorveglianza con dispositivi elettronici dell'imputato sottoposto a misure cautelari

New Technologies and Restriction of Personal Freedom: Electronic Surveillance of the Accused Placed under a Precautionary Measure

Novas tecnologias e restrições à liberdade pessoal: a vigilância com dispositivos eletrônicos do imputado submetido a medidas cautelares

Daniele Negri[1]

Università degli Studi di Ferrara - Italia

daniele.negri@unife.it

http://orcid.org/0000-0001-9162-4668

Abstract: Il contributo mette in luce l'ambiguità del rapporto fra la sorveglianza con dispositivi elettronici dell'imputato sottoposto a misura cautelare e il principio del sacrificio minimo della libertà personale, dissipando il corrente stereotipo circa la idoneità di tali dispositivi a favorire un minor ricorso alla custodia in carcere. Oltre a ciò, la continua evoluzione tecnica dei dispositivi di sorveglianza rischia di far degradare la dignità della persona. Altra questione messa in luce dall'autore riguarda il trattamento al quale sottoporre il singolo imputato nel caso in cui la pubblica amministrazione non sia in grado di garantire un numero sufficiente di dispositivi elettronici. La conclusione è nel senso che, in assenza di apparecchiature disponibili il giudice dovrà scegliere la misura degli arresti domiciliari, più mite della custodia in carcere, per non violare il divieto di eccesso nella restrizione della libertà personale.

Parole chiave: Sorveglianza elettronica; Libertà personale dell'imputato; Misure cautelari.

[1] Professore ordinario di Diritto processuale penale.

Abstract: *The paper highlights the ambiguity of the relationship between electronic surveillance of the accused subject to precautionary measures and the principle of minimum sacrifice of personal freedom, dissipating the current stereotype about the suitability of such devices to encourage less use of custody in prison. Furthermore, the continuous technical evolution of surveillance devices risks degrading the dignity of the person. Another issue underlined by the author concerns the treatment to which the individual accused must be subjected in case in which the public administration is unable to guarantee a sufficient number of electronic devices. The conclusion is that, in the absence of available equipment, the judge will have to choose the measure of house arrest, which is milder than custody in prison, in order not to violate the prohibition of excess in the restriction of personal freedom.*

Keywords: *Electronic surveillance; Personal freedom of the accused; Precautionary measures.*

Resumo: *O artigo evidencia a ambiguidade das relações entre a vigilância com dispositivos eletrônicos do imputado submetido a medidas cautelares e o princípio da restrição mínima à liberdade pessoal, dissipando o frequente estereótipo em relação à idoneidade de tais dispositivos para reduzir o encarceramento. No entanto, a contínua evolução técnica dos dispositivos de vigilância corre o risco de degradar a dignidade da pessoa. Outra questão pertinente refere-se ao tratamento a que se submete o imputado no caso em que a administração pública não é capaz de garantir um número suficiente de dispositivos eletrônicos. A conclusão é no sentido de que, se não houver aparelhos disponíveis, o juiz terá que determinar a medida de prisão domiciliar, menos aflitiva em relação à prisão em um instituto penitenciário, para não violar a proibição de excesso na restrição da liberdade pessoal.*

Palavras-chave: *Vigilância eletrônica; liberdade pessoal do imputado; medidas cautelares.*

1. *Innovazioni tecnologiche e sicurezza sociale*. Da almeno vent'anni a questa parte, su scala mondiale, prevale la tendenza delle legislazioni penali a cercare nella tecnologia più evoluta la carta vincente della strategia di politica criminale nevroticamente improntata all'incremento della sicurezza per la collettività. Se l'impiego massiccio dello strumentario penale a fini di prevenzione è un *tòpos* dei nostri tempi[2], indubbio è pure il contributo formidabile che a questo slittamento funzionale deriva dalla possibilità per gli Stati di confidare nelle prodigiose capacità anticipatorie della tecnica applicata al controllo sociale.

Il processo penale e la fase preliminare delle indagini, in particolare, hanno preso le sembianze di una gigantesca raccolta di dati personali tramite l'uso intensivo di sofisticate e occulte apparecchiature elettroniche, allo scopo di prevedere e neutralizzare con rapidità, prima che accadano, i comportamenti illeciti di persone ritenute pericolose[3]. Il bisogno immediato di sicurezza dei cittadini viene dunque appagato con la precoce restrizione del singolo individuo sottoposto ad indagini penali[4], risultato al quale si prestano le misure cautelari applicate durante il processo per evitare l'inquinamento probatorio, la fuga e – soprattutto – la commissione di reati[5]. È in questo scenario, dominato dal tentativo parossistico di chiudere ogni lacuna nella sempre più fitta rete dei dispositivi di sicurezza, che la tecnologia fa il suo ingresso anche tra le forme di limitazione anticipata della libertà personale e il controllo a distanza dell'imputato con mezzi elettronici gioca il ruolo di amplificatore di intensità della tutela cautelare.

---

2 HASSEMER, Winfried. Sicherheit durch Strafrecht. In: Strafverteidiger, p. 322 ss., 2006.

3 Cfr., volendo, NEGRI, Daniele. La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico). In: Archivio penale, n. 1, p. 44 ss., 2016. https://doi.org/10.12871/97888674166084. NEGRI, Daniele. Il processo penale come scriminante. In: *Revista brasileira de ciências criminais*, v. 101, p. 13 ss., 2013.

4 Parla al riguardo di «*Sicherheit durch Sicherung*», KAISER, Anna. *Durch Schritt und Tritt – die elektronische Aufenthaltsüberwachung:* Entwicklung, Rechtsgrundlagen, Verfassungsmäßigkeit. Wiesbaden: Springer, 2016, p. 64. https://doi.org/10.1007/978-3-658-14347-3.

5 Definisce la custodia cautelare in carcere come «vero avamposto della tutela sociale contro il pericolo», VIGANÒ, Francesco. Terrorismo, guerra e sistema penale. In: *Rivista italiana di diritto e procedura penale*, n. 2, p. 695, 2006.

Sono note le principali critiche rivolte contro questo fenomeno sin dalla sue origini. Per un verso si denuncia la commercializzazione dei poteri di controllo penale, visto che lo Stato è costretto ad acquistare sul mercato la tecnologia necessaria, affidando l'installazione dei dispositivi elettronici e il monitoraggio del loro funzionamento ad imprese private specializzate nel settore[6]. Per altro verso si paventa il rischio che l'individuo, vincolato a portare sempre addosso un'apparecchiatura munita di enormi potenzialità di intrusione nella sfera riservata, finisca così assoggettato ad un'attività di sorveglianza totale, in violazione dei più basilari principi costituzionali a salvaguardia della persona[7]. Infine, viene biasimato il potenziale effetto cosiddetto di *Net-Widening*, ossia la tentazione d'allargare progressivamente l'ambito dei soggetti sottoposti a controllo elettronico oltre quanto sarebbe necessario e giustificato, una volta che strumenti di tale portata siano resi facilmente disponibili all'autorità giudiziaria[8].

Di fronte a censure tanto gravi, almeno in parte avvalorate dall'esperienza, diviene allora cruciale la verifica del rispetto delle condizioni affinché il controllo a distanza mantenga la promessa originaria di fungere da congegno *pro libertate*: il pronostico era che sostituisse in molti casi l'applicazione della più afflittiva misura della custodia in carcere, evitando all'imputato le conseguenze dannose – dirette e indirette – dell'ingresso tra le mura degli istituti di detenzione. In questo senso risulta particolarmente istruttiva la parabola susseguente all'introduzione della sorveglianza elettronica nel sistema cautelare dell'ordinamento italiano. Cercheremo qui di mettere in luce, di quella singolare traiettoria, gli aspetti più strettamente connessi alle grandi e generali questioni sollevate dalla materia.

---

6 ALBRECHT, Hans-Jörg; ARNOLD, Harald; SCHÄDLER, Wolfram. Der hessische Modellversuch zur Anwendung der „elektronischen Fußfessel": Darstellung und Evaluation eines Experiments. In: *Zeitschrift für Rechtpolitik*, v. 33, p. 466 ss., 2000.

7 KRAHL, Matthias. Der elektronisch überwachte Hausarrest. In: *Neue Zeitschrift für Strafrecht*, n. 10, p. 461, 1997.

8 HAVERKAMP, Rita. Das Projekt „Elektronische Fußfessel" in Frankfurt am Main. In: *Bewährungshilfe*, n. 2, p. 166, 2003.

2. *Custodia in carcere come* extrema ratio*: fallimento di un obiettivo.* La modalità di controllo della persona accusata tramite mezzi elettronici si è inserita al principio di questo secolo (2000)[9] nel panorama e nelle dinamiche applicative delle misure cautelari personali, che il codice di procedura penale italiano (1989) aveva delineato un decennio prima con estrema cura sistematica. Presunzione di innocenza dell'imputato fino a condanna definitiva e inviolabilità della libertà personale sono le coordinate costituzionali ispiratrici di quella scrupolosa disciplina: al giudice la legge presenta un catalogo di strumenti tipici tra i quali scegliere, graduati in rapporto al livello di restrizione della sfera giuridica individuale. La custodia in carcere figura bensì al vertice della scala, ma, per l'appunto, non è più l'unica misura disponibile come accadeva sotto il codice previgente (1930); gli arresti domiciliari la seguono nell'ordine discendente, che conduce via via fino al divieto di espatrio, la più mite tra le misure coercitive, allargandosi altresì ad alcuni istituti di natura soltanto interdittiva.

Quest'assetto normativo corrisponde alla finalità di garanzia consistente nell'infliggere all'imputato, per le esigenze legate al perseguimento penale, il minore sacrificio necessario sulla base dei canoni di adeguatezza (rispetto alla natura e al grado del *periculum libertatis*) e di proporzionalità (in rapporto all'entità della pena pronosticabile) della misura cautelare da adottare nel caso concreto[10]. La custodia in carcere, dunque, è pensata dall'ordinamento processuale penale come soluzione estrema, attingibile solo quando ogni altra meno gravosa per l'individuo si riveli inidonea.

La realtà impietosa della giustizia penale praticata ha smentito clamorosamente il disegno razionale del codice, compiendo l'esatto contrario di quanto progettato dal legislatore. Nell'esperienza quotidiana è stata tradita l'aspettativa di contenere l'uso della carcerazione preventiva grazie alla pluralità dei mezzi cautelari, vista l'applicazione tutt'affatto marginale che hanno avuto le altre misure del catalogo. Il largo predominio statistico della massima coercizione personale risulta attestato, e al tempo stesso stigmatizzato, in una fondamentale

[9] D.l. 24 novembre 2000, n. 341, convertito in legge 19 gennaio 2001, n. 4.

[10] Corte cost., 21 luglio 2010, n. 265.

decisione della Corte europea dei diritti dell'uomo[11], che ha condannato lo Stato italiano per le disfunzioni strutturali alla base dell'ormai cronico sovraffollamento carcerario.

Nel giudicare alla stregua di trattamento inumano e degradante l'angusto spazio vitale riservato ai singoli detenuti, la Corte di Strasburgo esortava a privilegiare le misure alternative al carcere quale rimedio atto a ridurre la popolazione degli istituti penitenziari, mostrandosi particolarmente colpita dalla percentuale molto alta di persone ristrette a titolo cautelare e cioè a prescindere dalla pronuncia nei loro confronti di alcuna sentenza irrevocabile di condanna. In quel momento (2013) il rapporto tra persone relegate in carcere durante il processo e numero totale di detenuti era pari al 40%, ma una rappresentazione indicativa dell'entità del fenomeno proviene dai dati che si registrarono una ventina d'anni prima, al culmine delle inchieste giudiziarie per corruzione della classe politica e imprenditoriale divenute famose sotto il nome di "Mani pulite", quando l'ammontare degli imputati assoggettati alla misura cautelare più afflittiva giunse al tragico primato di sopravanzare addirittura – e non di poco – quello dei reclusi in esecuzione di pena[12].

I moniti della giurisprudenza sopranazionale si affiancano, del resto, alle molteplici raccomandazioni del Comitato dei Ministri del Consiglio d'Europa, anch'esse preordinate a circoscrivere l'applicazione della custodia in carcere ai casi di stretta necessità, a ridurne la durata al minimo compatibile con gli interessi della giustizia, a vietarne l'uso a scopi punitivi[13]. E proprio nella sorveglianza elettronica la Raccomandazione (2014) 4 scorge una sorta di panacea, poiché la diffusione dello strumento è ritenuta in grado di diminuire il tasso di ricorso alla privazione della libertà personale, lenendo la piaga del sovraffollamento carcerario senza per questo rinunciare al controllo efficace degli imputati pericolosi così da prevenirne le condotte illecite. Un rimedio che, al fine di conciliare al meglio le ragioni di garanzia individuale e le esigenze di difesa

[11] Corte e.d.u., 8 gennaio 2013, Torreggiani e altri c. Italia.

[12] Secondo i dati pubblicati dal Ministero della Giustizia, al 31 dicembre 1992 gli imputati in carcere erano pari al 132% nel rapporto con i condannati in esecuzione di pena.

[13] Cfr. Racc. (2006) 13 e Racc. (1999) 22.

sociale, dev'essere tuttavia – si ammette nello stesso documento – ben regolamentato e proporzionato.

3. *L'ambivalenza della sorveglianza elettronica: strumento* pro *o* contra libertatem*?* Questo insieme di sollecitazioni ha contribuito ai più recenti tentativi, da parte della legislazione italiana (2014-2015), di incentivare l'applicazione del monitoraggio tecnologico, risultata assai poco frequente nel quindicennio anteriore a causa della riluttanza dei giudici a convincersi che il controllo remoto possa scongiurare pericoli derivanti dallo stato di libertà dell'imputato paragonabili per intensità a quelli di solito fronteggiati con la custodia in carcere[14]; o, secondo una spiegazione più benevola, a motivo di un «colossale – quanto incomprensibile – difetto di informazione» dei magistrati circa la concreta possibilità di avvalersi del dispositivo[15]. Non è l'unico aspetto poco decifrabile di questa controversa partita, la cui posta in gioco è il primato della libertà individuale o il trionfo della sicurezza sociale.

Dalla prima comparsa e fino all'ultima modifica normativa, infatti, l'istituto della sorveglianza elettronica è vissuto su un'ambivalenza di fondo che ha alimentato l'ambiguità retorica intorno alla sua funzione: se, cioè, serva ad innalzare o ad abbassare mediamente il grado di limitazione della libertà personale; se migliori o peggiori, a livello statistico, il trattamento cautelare riservato agli imputati. Per rendersene conto basterà soffermarsi sull'antitesi che caratterizza, almeno in apparenza, le ragioni di politica criminale alla base delle principali riforme processuali in materia.

Il controllo elettronico venne introdotto (art. 275-*bis* c.p.p.) allo scopo di aumentare l'«efficacia» e l'«efficienza» nell'amministrazione della giustizia[16], corazzando la misura cautelare degli arresti domiciliari in modo

---

[14] In tal senso, v. NEGRI, Daniele. Tecniche di riduzione della custodia in carcere ad *extrema ratio*. In: CHINNICI, Daniela (a cura di). *Le misure cautelari personali nella strategia del "minimo sacrificio necessario"*. Roma: Dike, 2015, p. 52.

[15] BASSI, Alessandra; VON BORRIES, Christine. *Il braccialetto elettronico: un dispositivo dimenticato*. Disponibile in: *www.questionegiustizia.it*, 12 dicembre 2013.

[16] Il già citato d.l. n. 341 del 2000 divenne comunemente noto come decreto "antiscarcerazioni".

che l'imputato non potesse più trasgredire l'obbligo di permanenza tra le mura domestiche senza essere subito scoperto e presto neutralizzato. La vigilanza, discontinua nel tempo, del personale di polizia presso l'abitazione era sembrata troppo facilmente eludibile, specie a seguito dell'allarme sociale suscitato da alcune azioni delittuose di cui erano stati autori proprio soggetti sfuggiti agli arresti domiciliari[17].

Un intervento, dunque, volto a predisporre restrizioni ulteriori e più intense degli spazi di libertà individuale, accompagnate dal messaggio rassicurante all'opinione pubblica che la tecnologia sarebbe divenuta infallibile strumento di contrasto della criminalità. Nella prospettiva del legislatore la sorveglianza elettronica, insomma, non tanto rappresentava la soluzione idonea a favorire l'uso della custodia domestica in alternativa al carcere, quanto offriva l'opportunità di aggravare la condizione personale di chi, sulla scorta di un giudizio di adeguatezza della misura cautelare compiuto in assenza dei dispositivi tecnologici, sarebbe stato posto verosimilmente agli arresti domiciliari con le tradizionali modalità di controllo. Un esempio calzante di *Net-Widening*.

La giurisprudenza, a sua volta, ha assecondato questa chiara propensione *contra libertatem* traendo argomento dal «consenso» dell'imputato, fattore al quale il codice subordina la possibilità per il giudice di applicare gli arresti domiciliari nella particolare conformazione assistita dal monitoraggio tecnologico. La circostanza che il soggetto accetti di indossare il dispositivo elettronico e di essere quindi costantemente sorvegliato è presa a dimostrazione della volontà di autolimitare la propria libertà di movimento, ossia di resistere all'impulso di allontanarsi dall'abitazione al fine di delinquere. L'atto di sottomissione al congegno, sintomatica di un grado di pericolo attenuato, escluderebbe così che, per contenere adeguatamente la probabilità di realizzazione dell'evento temuto, sia necessario il ricorso alla misura estrema della custodia in carcere[18].

---

[17] CESARIS, Laura. Dal *panopticon* alla sorveglianza elettronica. In: BARGIS, Marta (a cura di). *Il decreto "antiscarcerazioni"*. Torino: Giappichelli, 2001, p. 54.

[18] Tra le altre, v. Cass., sez. II, 23 settembre 2014, Di Francesco e a. In: *C.e.d.*, n. 261439; Cass., sez. V, 19 giugno 2012, Bottan. In: *C.e.d.*, n. 253716; Cass., sez. II, 29 ottobre 2003, Bianchi. In: *C.e.d.*, n. 227582.

Ma ciò significa, alla fin fine e all'atto pratico, tramutare gli arresti domiciliari sorvegliati elettronicamente nella modalità ordinaria di esecuzione della tipologia di misura subito inferiore a quella massima per livello di afflittività, poiché vale anche il ragionamento inverso: se l'imputato non è chiamato a prestare il consenso, richiesto dalla legge soltanto quando il giudice intende applicare gli arresti domiciliari con vigilanza tecnologica, neppure viene messa alla prova l'inclinazione soggettiva a rispettare i vincoli della custodia più mite presso l'abitazione; sicché il giudice ha compito facile nel motivare l'esistenza di esigenze cautelari di intensità tanto elevata da rendere indispensabile la carcerazione preventiva. Gli arresti domiciliari non muniti di controllo a distanza diventano, a quel punto, un'alternativa difficilmente percorribile di fronte ad alti livelli di pericolosità dell'imputato.

Con il pretesto di diminuire il tasso di carcerazione preventiva, agevolando a questo fine l'uso di strumenti cautelari meno gravosi, il legislatore ha poi codificato negli esatti termini appena descritti (2014)[19] il rapporto tra gli arresti domiciliari accompagnati dalla sorveglianza elettronica e la stessa misura disposta senza alcuna previsione di controllo remoto. Oggi, il giudice che sia orientato a preferire la custodia domestica deve spiegare perché non reputa necessaria la contestuale imposizione del monitoraggio con mezzi tecnologici, mentre in precedenza aveva l'onere di motivare il provvedimento, sulla specifica questione del controllo a distanza, solo qualora ritenesse tale forma di coercizione supplementare indispensabile ad evitare pericoli concreti d'una certa entità.

L'esigenza di ridurre il sovraffollamento degli istituti penitenziari – come abbiamo già detto – è stata al centro anche della successiva riforma del 2015, animata dall'ambizioso progetto di limitare il largo predominio pratico della custodia in carcere ripristinando la logica del minore sacrificio necessario a carico della libertà personale dell'imputato. Nell'occasione, è stata riscritta pure la disciplina degli arresti domiciliari sorvegliati con l'ausilio della tecnologia. E di nuovo è emersa la doppiezza dell'istituto: una volta proclamato l'essenziale principio di residualità della custodia detentiva, il legislatore si è

[19] D.l. 23 dicembre 2013, n. 146, convertito in legge 21 febbraio 2014, n. 10.

affrettato a lanciare un segnale tranquillizzante agli occhi della collettività intimorita dalla prospettiva di assistere a numerose fuoriuscite dal carcere.

Così, il codice stabilisce ora che il giudice, quando sceglie di applicare la coercizione di grado massimo, debba indicare le ragioni per le quali non risulta idonea a fronteggiare le esigenze del caso concreto la misura degli arresti domiciliari rafforzata con il localizzatore a distanza. Questo comporta, da un lato, che occorre un particolare impegno giustificativo per applicare la custodia carceraria, onere funzionale – almeno sulla carta – ad arginarne la frequenza; dall'altro lato, però, che un imputato sull'orlo dell'incarcerazione, a causa della sua elevata pericolosità, è destinato a subire nel migliore dei casi la misura degli arresti domiciliari vigilati elettronicamente, essendo quest'ultima l'unica alternativa menzionata dal legislatore.

In definitiva, siamo indotti a considerare l'uso della sorveglianza tecnologica come opzione migliorativa per l'imputato soltanto perché si è consolidata l'idea, contraria ai principi della presunzione di innocenza e della inviolabilità della libertà personale, che la carcerazione nel corso del processo rappresenti la regola.

4. *Il ruolo dei principi di legalità e di proporzionalità.* L'irruzione delle nuove tecnologie in ambito cautelare pone un problema di rapporti tra fonti giuridiche. Sono infatti coinvolti beni fondamentali tutelati dalla Costituzione e dalla Convenzione europea dei diritti dell'uomo: in primo luogo la libertà personale, ma pure la vita privata e lo sviluppo delle relazioni sociali; sullo sfondo, campeggia l'esigenza di salvaguardare il nucleo incomprimibile della dignità della persona. Si comprende dunque la ragione per la quale la già menzionata Raccomandazione (2014) 4 del Comitato dei Ministri del Consiglio d'Europa stabilisce che non soltanto l'uso, ma anche i tipi, la durata e le modalità di esecuzione della sorveglianza elettronica debbano essere disciplinati dalla legge: occorre certezza sui limiti del potere e massima democraticità nel processo decisionale volto a fissarli.

Pecca invece di indeterminatezza la previsione del codice (art. 275-*bis*) che si limita ad autorizzare «procedure di controllo mediante mezzi elettronici o altri strumenti tecnici», senza specificarne i connotati.

Ci si affida in proposito ad un provvedimento del governo[20], il quale così chiarisce le caratteristiche del dispositivo: si tratta di un bracciale di «peso ridotto» da agganciare alla caviglia (ciò spiega la denominazione corrente di "braccialetto" elettronico), che funge da trasmettitore collegato mediante linea telefonica alle centrali operative dei corpi di polizia. Tale conformazione senza dubbio aiuta a ridurre le interferenze nelle relazioni familiari e sociali del sorvegliato, nonché a circoscrivere i rischi di stigmatizzazione dell'individuo quando sia autorizzato a muoversi nell'ambiente esterno all'abitazione, in quanto i gesti quotidiani non ne risulteranno impediti e il dispositivo potrà essere facilmente coperto alla vista di persone terze portando abiti lunghi alla caviglia così da impedire che l'imputato, presunto innocente, sia percepito dalla collettività come pericoloso criminale.

Essenziale è anche un'ulteriore indicazione contenuta nella Raccomandazione sopra citata, riguardante la necessità di revisione periodica delle regole sui mezzi di controllo a distanza «per tenere conto degli sviluppi tecnologici nel settore, in maniera tale da evitare un livello di intrusione eccessivo nella vita privata o familiare dei sospettati». La norma chiama in causa il principio di proporzionalità, considerando il relativo *test* in termini dinamici, fondato cioè su criteri non assoluti ma sempre aggiornati allo stato della scienza. Bisogna allora chiarire fino a che punto alla legge spetti il primato.

Da un lato, i limiti congeniti alla formulazione astratta della legge e i tempi solitamente lunghi che servono a modificarla per metterla al passo appaiono poco compatibili con lo scrupolo di dettaglio necessario a descrivere le caratteristiche degli apparati elettronici e con la velocità della loro evoluzione tecnica, tanto da rendere preferibile demandare il compito ad atti normativi di rango subordinato. Dall'altro lato, però, la legge non può sottrarsi al vincolo di dettare almeno i parametri essenziali e di fissare i divieti.

Quanto ai secondi, viene a tema l'ammissibilità dei *microchip* impiantati sottocute. Esempio emblematico di come l'evoluzione digitale consenta di rimpicciolire al massimo i trasmettitori e il progresso scientifico

[20] Decreto Ministro dell'interno del 2 febbraio 2001. In: *Gazzetta Ufficiale*, 15 febbraio 2001, n. 38.

riesca a renderli addirittura invisibili, annullando il potenziale stigma sociale che deriva all'imputato dal mostrarsi assoggettato al dispositivo di sicurezza senza creare rischi alla salute. Al tempo stesso, ripugna allo Stato costituzionale di diritto degradare la persona sino al punto di introdurre apparecchiature trasmittenti all'interno del corpo umano per gli scopi connessi all'attività di repressione penale, sicché la legge dovrebbe proibire con clausole generali operazioni simili anche qualora l'imputato acconsentisse a subirle: la minaccia implicita dell'ingresso in carcere, se non accettasse l'alternativa della sorveglianza elettronica, sembra sufficiente a viziare la volontà manifestata in tal senso.

L'altro aspetto sul quale la legge dovrebbe sempre esprimersi riguarda la tipologia di prestazioni dei dispositivi autorizzati, modulata in base al grado di intensità del controllo e alla natura dei diritti incisi. Desta attenzione il confronto tra i braccialetti elettronici di risalente produzione, che segnalavano mediante radiofrequenza soltanto la fuoriuscita del soggetto dall'area del domicilio, e i congegni dotati di sistema *GPS Tracking*, capace di seguire la persona in tutti i suoi spostamenti sul territorio.

La possibilità di avvalersi di questi ultimi e più progrediti apparecchi per finalità di tutela cautelare è stata introdotta nell'ordinamento processuale italiano senza un'apposita base legale, ma considerando sufficiente il generico rinvio del codice ai «mezzi elettronici» e agli «altri strumenti tecnici» previsti in abbinamento agli arresti domiciliari. Quando il legislatore ha deciso di estendere la modalità del controllo a distanza anche alla misura cautelare dell'allontanamento dalla casa familiare (2013)[21], così da potenziare la vigilanza sul rispetto delle relative prescrizioni, il governo si è limitato a stipulare una nuova convenzione con la società di telefonia concessionaria del servizio in virtù della quale una quota della fornitura di braccialetti elettronici va munita della funzione *GPS*[22]. Qui siamo addirittura di fronte alla eterointegrazione per via negoziale – cioè ad una forma di privatizzazione – di un elemento essenziale della fattispecie che regola l'intensità del potere cautelare.

---

[21] D.l. 14 agosto 2013, n. 93, convertito in legge 15 ottobre 2013, n. 119.

[22] Cfr. in proposito APRILE, Stefano. Il sistema per il controllo elettronico delle persone sottoposte alla misura degli arresti domiciliari previsto dall'art. 275-*bis*, c.p.p.: "braccialetto elettronico". L'esperienza del Gip di Roma. In: *Rassegna penitenziaria e criminologica*, n. 2, p. 55, 2013.

Il passaggio alla geolocalizzazione non è indifferente al fine di misurare la proporzionalità della pressione esercitata sulla sfera giuridica del singolo. Le grandezze da sottoporre a verifica, perciò, vanno chiaramente scandite dalla legge affinché non vengano lasciate alla discrezionalità incontrollata del giudice. Un conto, infatti, è la sorveglianza circoscritta all'interno d'un perimetro ben definito dalla legge, quando essa autorizza gli arresti presso l'abitazione. Tutt'altro discorso attiene al monitoraggio ininterrotto nel tempo di ogni movimento dell'imputato, osservato passo passo ovunque costui si trovi. Nel primo caso si controlla la mera situazione di presenza della persona all'interno di un unico spazio predeterminato; nel secondo, oltre alla costante rintracciabilità del soggetto, si ottiene una miriade di informazioni sulle sue abitudini di vita attraverso la mappatura dei luoghi che frequenta.

Non è detto che tale messe di informazioni serva agli scopi per i quali il giudice ha impartito l'ordine di non avvicinarsi a certi luoghi o persone; quei dati non rilevano fintanto che il divieto non venga violato e solo nella porzione che registra la trasgressione; di conseguenza, la tecnologia usata per il controllo a distanza comporta un eccesso di sacrificio individuale che la legge non può trascurare, abilitando il giudice all'impiego dello strumento soltanto a determinate condizioni e predisponendo i rimedi di natura successiva (modi e tempi di conservazione dei dati, apparato sanzionatorio). Se poi – poniamo, ma è eventualità nient'affatto remota oggigiorno – il dispositivo venisse dotato d'una minuscola videocamera collegata alle postazioni di polizia e attivabile d'autorità, l'*escalation* nelle potenzialità tecnologiche applicate al controllo sociale aprirebbe lo scenario orwelliano della sorveglianza integrale. Non è allora pensabile che la legge si astenga dal dettare precisi limiti negativi al riguardo e, là dove certe tipologie di sorveglianza non vengano del tutto escluse, dal differenziare i presupposti applicativi a seconda del grado di intrusione nelle libertà della persona.

Il principio di proporzionalità rileva in materia pure sotto il profilo che attiene al bilanciamento tra il livello di compressione della sfera giuridica individuale e la gravità del reato perseguito. Da quest'angolazione l'ordinamento processuale italiano mostra vistosi cedimenti. In particolare, essi riguardano le recenti novelle legislative

concepite all'insegna della crescente centralità nella tutela della vittima[23], che hanno portato dapprima ad arricchire la gamma dei mezzi cautelari con le misure dell'allontanamento dell'imputato dalla casa familiare e del divieto di avvicinarsi ai luoghi frequentati dalla persona offesa dal reato; in seguito (2013, 2019)[24] a prevedere la possibilità per il giudice di rafforzare le medesime misure tramite la sorveglianza elettronica, necessariamente eseguita tramite localizzatore *GPS* visto che l'imputato destinatario di quei provvedimenti d'interdizione all'ingresso in certi spazi resta libero per il resto di circolare sul territorio.

Ebbene, di norma simili restrizioni della libertà di movimento sono autorizzate dalla legge quando oggetto del procedimento penale sia un delitto punito con la reclusione superiore nel massimo edittale a tre anni. Sono le eccezioni al ribasso, rispetto a questa soglia sanzionatoria, a mettere in dubbio la correttezza del contemperamento tra i due interessi in gioco, nel momento in cui l'imputato non soltanto è reso destinatario di proibizioni, ma diviene passibile di localizzazione permanente e dunque subisce un aggravio della propria condizione soggettiva. In particolare, alcune fattispecie di reato contemplate nell'elenco di quelle derogatorie alla disciplina ordinaria (ad esempio, la violazione degli obblighi di assistenza familiare, l'abuso dei mezzi di correzione, la minaccia) non appaiono di tale disvalore, come attesta anche il livello inferiore di pena edittale, da giustificare la legittimazione a disporre che l'imputato porti sempre addosso il braccialetto elettronico equipaggiato con tracciamento *GPS*.

5. *Costi della tecnologia e inviolabilità della libertà personale*. Una vicenda dai tratti grotteschi, verificatasi nell'ambito della giustizia penale italiana, suscita riflessioni serie sul nodo cruciale del rapporto tra diritto e progresso tecnologico riguardante le conseguenze per l'individuo che non possa beneficiare dei nuovi mezzi a causa della scarsità di esemplari dovuta al loro costo. Per il nostro tema specifico, il quesito può essere così riformulato. Posto che, nell'attuale sistema cautelare, la sorveglianza

[23] Nel 2013 erano attivi 55 braccialetti in totale: BASSI, Alessandra; VON BORRIES, Christine. *Il braccialetto elettronico: un dispositivo dimenticato*. Disponibile in: *www.questionegiustizia.it*, 12 dicembre 2013.

[24] Da ultimo, legge 19 luglio 2019, n. 69.

elettronica funge da presidio degli arresti domiciliari in grado di scongiurare la custodia in carcere, quale trattamento subisce la libertà dei singoli imputati se l'autorità non è rifornita di apparecchiature sufficienti ad esaurire tutti i casi in cui i giudici valutino adeguata e proporzionata la misura domestica controllata a distanza? Il problema è stato presagito ma non affrontato dal legislatore, il quale, nell'attribuire il potere di applicazione del controllo mediante strumenti tecnici, ha semplicemente aggiunto al testo del codice una clausola prudenziale: «quando» il giudice «ne abbia accertato la disponibilità da parte della polizia giudiziaria» (art. 275-*bis* c.p.p.).

Se si eccettua il primo periodo di sperimentazione circoscritta a pochi uffici giudiziari, il numero di braccialetti elettronici in dotazione è cresciuto nel decennio 2003-2013 fino a circa duemila esemplari a seguito del rinnovo della convenzione tra governo e società privata gestrice del servizio. La regolarità della procedura che ha portato alla scelta dell'impresa fornitrice è stata contestata davanti alla giustizia amministrativa da un'azienda concorrente; ma ciò che più colpisce è il costo risultato esorbitante della strumentazione a fronte del suo scarsissimo uso[25], tanto da portare alla censura da parte della Corte dei Conti[26]. Le riforme degli anni successivi e, in particolare, la possibilità di impiego del braccialetto elettronico per la sorveglianza di imputati anche al di fuori dell'abitazione sono all'origine del notevole aumento della domanda che ha evidenziato la drammatica carenza di apparecchiature disponibili.

È a quel punto che nasce la disputa sulla sorte degli imputati destinatari del provvedimento degli arresti domiciliari vigilati a distanza. Un primo indirizzo giurisprudenziale propendeva per l'adozione della custodia in carcere, dato che l'alta pericolosità dell'imputato non sarebbe stata neutralizzabile con la più tenue modalità della sorveglianza saltuaria

---

[25] Fino al 2013 erano stati spesi oltre 81 milioni di euro; il costo giornaliero per ogni braccialetto risultava pari a 115 euro. Il quadro di questa disastrosa esperienza è ricostruito in VALENTINI, Elena. Arresti domiciliari e indisponibilità del braccialetto elettronico: è il momento delle Sezioni Unite. Disponibile in: *www.penalecontemporaneo.it*, 27 aprile 2016, p. 3; GRASSIA, Rosa Gaia. Il braccialetto elettronico: uno strumento inespresso. Quando la tecnologia è al servizio dell'uomo, ma la copertura finanziaria non è al servizio della tecnologia. In: *Archivio penale (web)*, n. 3, p. 4, 2015.

[26] Deliberazione n. 11/2012/G.

di polizia presso l'abitazione[27]. Un secondo orientamento, al contrario, metteva l'accento sulla natura solo accessoria del controllo elettronico rispetto agli arresti domiciliari, ritenendo che la valutazione di adeguatezza a fronteggiare le esigenze cautelari del caso concreto avesse comunque per riferimento quel tipo di misura, a prescindere dalla dotazione del supporto tecnologico.

In posizione intermedia si collocava la soluzione di trattenere l'imputato in carcere fino a quando non fosse sopravvenuta la materiale disponibilità del braccialetto elettronico. Venivano così a formarsi liste d'attesa la cui gestione finiva per dipendere in pratica dall'azienda addetta all'installazione dei congegni, con grave difetto di trasparenza sulle graduatorie e i criteri di priorità[28]. Lo spettro inquietante della privatizzazione delle misure limitative della libertà personale si è dunque materializzato, anche se alcuni uffici giudiziari avevano dettato minime direttive in proposito come quella di privilegiare, nell'accesso al braccialetto elettronico, gli imputati già ristretti in carcere (cosiddetta opzione *Backdoor*) a scapito di chi fosse in procinto di entrarvi (sistema *Frontdoor*)[29]. Ciò dava luogo a disparità di trattamento irragionevoli[30], dovute a inefficienze e ristrettezze finanziarie della pubblica amministrazione, incapace di garantire provviste adeguate al bisogno.

Va colta qui la manifestazione specifica di un interrogativo più generale legato al canone di proporzionalità: se, cioè, l'esito della valutazione sul minimo sacrificio necessario da imporsi alla libertà individuale risenta del fatto che la selezione di un mezzo più mite comporterebbe costi considerevolmente maggiori a carico dello Stato. La

---

[27] Cass., sez. II, 10 novembre 2015, Pappalardo e a. In: *C.e.d.*, n. 265238; Cass., sez. II, 19 giugno 2015, Candolfi. In: *C.e.d.*, n. 264230.

[28] BASSI, Alessandra; VON BORRIES, Christine. Il braccialetto elettronico fra luci ed ombre. In: *Cassazione penale*, n. 9, p. 3132 ss., 2016.

[29] LEONARDI, Fabrizio. La sorveglianza elettronica come alternativa al carcere: l'esperienza europea. In: *Rassegna penitenziaria e criminologica*, n. 2, p. 88, 2013.

[30] VALENTINI, Elena. Arresti domiciliari e indisponibilità del braccialetto elettronico: è il momento delle Sezioni Unite. Disponibile in: *www.penalecontemporaneo.it*, 27 aprile 2016, p. 17. Ma v. già MARZADURI, Enrico. Commento all'art. 16 d.l. 24 novembre 2000, n. 341 – Efficienza della giustizia. In: *La legislazione penale*, n. 1-2, p. 449, 2001.

Corte di cassazione italiana ha risolto la questione ritenendo inesigibile dallo Stato l'acquisto di un numero di braccialetti elettronici pari a quello degli imputati che ne avrebbero diritto, poiché le risorse della pubblica amministrazione sono necessariamente limitate e così le prestazioni (ad esempio, sanitarie, scolastiche) erogate ai cittadini[31]. Della conclusione sembra tuttavia lecito dubitare. E non soltanto perché ripugna immiserire l'alto valore della tutela della persona a meschino affare di denaro[32]. L'argomento speso dalla Corte, infatti, confonde le prestazioni positive di cui è gravato lo Stato sociale, senz'altro condizionate dal bilancio, con la libertà negativa riconosciuta come inviolabile a tutti gli individui[33]. La supremazia assiologica conferita dalla Costituzione alla sfera intangibile del singolo comporta che il rischio di fallimento della strategia cautelare ricada sull'autorità: in assenza di apparecchiature disponibili il giudice dovrà quindi scegliere la misura più mite degli arresti domiciliari per non violare il divieto di eccesso nella restrizione della libertà personale, trasgressione che invece si avrebbe applicando la custodia carceraria in quanto sovradimensionata rispetto all'entità del pericolo da elidere nel caso concreto.

Per le stesse ragioni non è condivisibile il responso che la Corte di cassazione, a sezioni unite, ha dato alla diatriba giurisprudenziale. Sostiene la Corte che, quando il giudice abbia dapprima ritenuto adeguati gli arresti domiciliari controllati a distanza, ove poi emergesse l'indisponibilità del braccialetto elettronico dovrebbe dare atto della impossibilità di applicare la misura più idonea e compiere di nuovo la valutazione di adeguatezza mediante il bilanciamento tra il grado delle esigenze cautelari e la necessità di salvaguardia della libertà

---

31 Cass., sez. II, 17 settembre 2014, n. 520, *inedita* (ma in: *De Jure*).

32 Così, MAIWALD, Manfred, § 100a StPO. In: WASSERMANN, Rudolf (a cura di), *Alternativkommentar zur Strafprozeßordnung*. Neuwied: Luchterhand, 2ª ed., v. II, tomo I, 1992, n.m. 8; *contra*, BLOZIK, Michael. *Subsidiaritätsklauseln im Strafverfahren*. Göttingen: Universitätsverlag Göttingen, 2012, p. 147. https://doi.org/10.17875/gup2012-143.

33 Nel senso che le carenze della pubblica amministrazione non possano mai giustificare la privazione della libertà personale, v. anche CASSIBBA, Fabio. L'indisponibilità del "braccialetto elettronico": le Sezioni Unite escludono automatismi decisori ma residuano dubbi. In: *Processo penale e giustizia*, n. 5, p. 181, 2016.

personale[34]. In verità l'esito della ponderazione è vincolato dalle coordinate costituzionali. Se inizialmente il giudice reputa eccessiva la custodia in carcere, tanto da prediligere la misura meno grave degli arresti domiciliari tecnologicamente sorvegliati, disporre in seguito la restrizione intramuraria per mancanza di congegni significa tollerare una quota marginale di sacrificio della libertà personale palesemente priva di giustificazione e dunque illegittima.

Bibliografia

ALBRECHT, Hans-Jörg; ARNOLD, Harald; SCHÄDLER, Wolfram. Der hessische Modellversuch zur Anwendung der „elektronischen Fußfessel": Darstellung und Evaluation eines Experiments. In: *Zeitschrift für Rechtpolitik*, v. 33, p. 466-469, 2000.

APRILE, Stefano. Il sistema per il controllo elettronico delle persone sottoposte alla misura degli arresti domiciliari previsto dall'art. 275-*bis*, c.p.p.: "braccialetto elettronico". L'esperienza del Gip di Roma. In: *Rassegna penitenziaria e criminologica*, n. 2, p. 47-71, 2013.

BASSI, Alessandra; VON BORRIES, Christine. Il braccialetto elettronico fra luci ed ombre. In: *Cassazione penale*, n. 9, p. 3127-3139, 2016.

BASSI, Alessandra; VON BORRIES, Christine. *Il braccialetto elettronico: un dispositivo dimenticato*. Disponibile in: *www.questionegiustizia.it*, 12 dicembre 2013.

BLOZIK, Michael. Subsidiaritätsklauseln im Strafverfahren. Göttingen: Universitätsverlag Göttingen, 2012. https://doi.org/10.17875/gup2012-143.

CASSIBBA, Fabio. L'indisponibilità del "braccialetto elettronico": le Sezioni Unite escludono automatismi decisori ma residuano dubbi. In: *Processo penale e giustizia*, n. 5, p. 175-182, 2016.

CESARIS, Laura. Dal *panopticon* alla sorveglianza elettronica. In: BARGIS, Marta (a cura di). *Il decreto "antiscarcerazioni"*. Torino: Giappichelli, 2001, p. 49-79.

GRASSIA, Rosa Gaia. Il braccialetto elettronico: uno strumento inespresso. Quando la tecnologia è al servizio dell'uomo, ma la copertura finanziaria non è al servizio della tecnologia. In: *Archivio penale (web)*, n. 3, 2015.

[34] Cass., sez. un., 28 aprile 2016, Lovisi. In *C.e.d.*, n. 266651.

HASSEMER, Winfried. Sicherheit durch Strafrecht. In: *Strafverteidiger*, p. 321-332, 2006.

HAVERKAMP, Rita. Das Projekt „Elektronische Fußfessel“ in Frankfurt am Main. In: *Bewährungshilfe*, n. 2, p. 164-181, 2003.

KAISER, Anna. *Durch Schritt und Tritt – die elektronische Aufenthaltsüberwachung:* Entwicklung, Rechtsgrundlagen, Verfassungsmäßigkeit. Wiesbaden: Springer, 2016. https://doi.org/10.1007/978-3-658-14347-3.

KRAHL, Matthias. Der elektronisch überwachte Hausarrest. In: *Neue Zeitschrift für Strafrecht*, n. 10, p. 457-461, 1997.

LEONARDI, Fabrizio. La sorveglianza elettronica come alternativa al carcere: l'esperienza europea. In: *Rassegna penitenziaria e criminologica*, n. 2, p. 79-124, 2013.

MAIWALD, Manfred, § 100a StPO. In: WASSERMANN, Rudolf (a cura di), *Alternativkommentar zur Strafprozeßordnung*. Neuwied: Luchterhand, 2ª ed., v. II, tomo I, 1992.

MARZADURI, Enrico. Commento all'art. 16 d.l. 24 novembre 2000, n. 341 – Efficienza della giustizia. In: *La legislazione penale*, n. 1-2, p. 445-453, 2001.

NEGRI, Daniele. Il processo penale come scriminante. In: *Revista brasileira de ciências criminais*, v. 101, p. 13 -50, 2013.

NEGRI, Daniele. La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico). In: *Archivio penale*, n. 1, p. 44-54, 2016. https://doi.org/10.12871/97888674166084.

NEGRI, Daniele. Tecniche di riduzione della custodia in carcere ad *extrema ratio*. In: CHINNICI, Daniela (a cura di). *Le misure cautelari personali nella strategia del "minimo sacrificio necessario"*. Roma: Dike, 2015, p. 39-70.

VALENTINI, Elena. Arresti domiciliari e indisponibilità del braccialetto elettronico: è il momento delle Sezioni Unite. Disponibile in: *www.penalecontemporaneo.it*, 27 aprile 2016.

VIGANÒ, Francesco. Terrorismo, guerra e sistema penale. In: *Rivista italiana di diritto e procedura penale*, n. 2, p. 648-703, 2006.

Informações adicionais e declarações dos autores
(integridade científica)

Declaração de conflito de interesses (conflict of interest declaration): o autor confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores.

Declaração de ineditismo e originalidade (declaration of originality): o autor assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 02/09/2019
- Controle preliminar e verificação de plagio: 06/09/2019
- Avaliação 1: 16/09/2019
- Avaliação 2: 02/10/2019
- Decisão editorial preliminar: 03/10/2019
- Retorno rodada de correções: 05/10/2019
- Decisão editorial final: 08/10/2019

Equipe editorial envolvida:
- Editor-chefe: 1 (VGV)
- Editoras-associadas: 2 (CC e BC)
- Revisores: 2

COMO CITAR ESTE ARTIGO:

NEGRI, Daniele. Nuove tecnologie e compressione della libertà personale: la sorveglianza con dispositivi elettronici dell'imputato sottoposto a misure cautelari. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1255-1275, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.289

L'acquisizione delle prove digitali dai *service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale

Digital Evidence gathering from service providers: a worrying paradigm shift in international cooperation

Obtenção de provas digitais por servidores: uma preocupante mudança de paradigma na cooperação internacional

Marcello Daniele[1]

Università degli Studi di Padova - Italia

marcello.daniele@unipd.it

http://orcid.org/0000-0002-8791-255X

Abstract: È sempre più frequente che le prove digitali rilevanti ai fini di un procedimento penale non siano localizzate nello Stato di commissione del reato, ma si trovino disperse nel *cloud*, risultando accessibili solo grazie all'intervento dei *service provider* che le detengono. In casi del genere i tradizionali strumenti di cooperazione giudiziaria entrano in crisi, poiché può diventare molto difficile individuare uno Stato di esecuzione a cui rivolgere le richieste istruttorie. Di qui l'idea, recepita da una proposta di regolamento dell'Unione Europea, di creare un canale di cooperazione diretta fra le autorità giudiziarie interessate all'acquisizione delle prove e i *provider*, a cui spetterebbe verificare che le richieste istruttorie rispettino la Carta di Nizza. Ne deriverebbe, però, la privatizzazione di un'attività tradizionalmente riservata ad organi pubblici: un preoccupante cambio di paradigma che rischia di porre in serio pericolo i diritti fondamentali.

Parole chiave: Prova digitale; cooperazione giudiziaria; diritti fondamentali.

[1] Professore ordinario di Diritto processuale penale.

Abstract: *It is becoming increasingly common that digital evidence relevant to criminal proceedings is not located in the State in which the crime was committed, but it is spread in the cloud computing, and it can be accessed only thanks to the intervention of the service providers that hold it. In such cases traditional instruments of judicial cooperation enter into crisis, since it can become very difficult to identify an executing State to which the evidence requests can be addressed. Hence the idea, implemented by a proposal for a European Union regulation, to create a channel of direct cooperation between the judicial authorities interested in acquiring the evidence and the providers, who would be responsible for verifying that the evidence requests respect the Charter of Nice. The result, however, is the privatization of an activity traditionally reserved to public bodies: a worrying paradigm shift that could put fundamental rights in serious danger.*

Keywords: *Digital Evidence; Judicial cooperation; fundamental rights.*

Resumo: *É cada vez mais frequente que as provas digitais relevantes para um processo penal não sejam localizadas no Estado em que ocorreu o cometimento de um crime, e que se encontrem dispersas no cloud, tornando-se dessa forma acessíveis somente por meio da intervenção do service provider que realiza o armazenamento. Nesses caos, os tradicionais instrumentos de cooperação judiciária entram em crise, porque pode tonar-se muito difícil especificar um Estado de execução ao qual direcionar pedidos de cooperação. Nesse quadro delineado, nasce a ideia, acolhida em uma proposta de regulamentação da União Europeia, de criar um canal de cooperação direta entre as autoridades judiciarias interessadas na colheita da prova e o provider, ao qual caberia verificar se os pedidos instrutórios respeitam a Carta de Nice. No entanto, trata-se de tendência de privatização de uma atividade tradicionalmente reservada aos órgãos públicos: uma preocupante mudança de paradigma capaz de fragilizar os direitos fundamentais.*

Palavras-chave: *Prova digital; cooperação judiciária; direitos fundamentais.*

1. Le prove digitali disperse nel *cloud*.

Non è raro che le prove digitali rilevanti ai fini di un procedimento penale si trovino in uno Stato diverso da quello di commissione del reato[2], sfuggendo così alla sovranità esclusiva di quest'ultimo. È una situazione a cui gli strumenti della cooperazione internazionale non riescono a rimediare, nella misura in cui – come sempre più spesso accade – si tratti di prove che circolano nello spazio virtuale del *cloud*[3], detenute da *service provider*: aziende private che offrono i più vari prodotti *online* (*email*, *social network*, *hosting*) a livello globalizzato, e la cui collaborazione si rivela, così, imprescindibile ai fini delle indagini. In alternativa, gli organi investigativi dovrebbero acquisire le prove con mezzi propri (ad esempio, tramite l'inoculazione di un *trojan* in un dispositivo in cui si presume che esse siano reperibili); con il rischio, però, di danneggiarle o contraffarle, pregiudicandone la spendibilità in giudizio[4].

Di qui l'esigenza di rimeditare il postulato – finora dato per scontato – secondo cui la cooperazione dovrebbe avvenire fra organi statali. Diventa indispensabile pensare a meccanismi in grado di includere anche i *provider*; ed è un compito non facile, se si considera che, come vedremo, richiede di coinvolgere in attività a rilevanza pubblica soggetti privati che, coadiuvando le autorità inquirenti, potrebbero rischiare di pregiudicare i propri interessi.

2. La cooperazione fra organi statali: una soluzione insoddisfacente.

Come è noto, gli attuali strumenti di cooperazione – la rogatoria e, nell'ambito dell'Unione Europea, la sua versione più evoluta, rappresentata

---

[2] Su questa loro caratteristica, v. M. Daniele, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 285 s., e S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 152 s.

[3] Cfr., al riguardo, S. Aterno, *Cloud forensics: aspetti giuridici e tecnici*, in Aa.Vv., *Cybercrime*, dir. da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Utet, 2019, p. 1689 s.

[4] V. L. Bartoli, *Digital evidence for the criminal trial: limitless cloud and state boundaries, in Big data and Public Law: new challenges beyond data protection*, in *rivista.eurojus.it*, num. spec., 2019, p. 102.

dall'ordine europeo di indagine penale (OEI) [5] – sono fondati sulla collaborazione fra i competenti organi investigativi degli Stati coinvolti nelle operazioni istruttorie: lo Stato di emissione della richiesta, in cui vige la *lex fori*, e lo Stato di esecuzione, ossia quello in cui la prova è reperibile, in cui vale la *lex loci*. Così operando, però, non offrono una risposta soddisfacente al problema dell'acquisizione delle prove digitali nel *cloud*.

Anzitutto a causa della loro lentezza. Le norme che li regolano sono state concepite per le prove fisiche, e non sempre prevedono tempistiche di trasmissione adatte alla velocità con cui le prove digitali si muovono nella rete e possono trasmigrare da uno Stato ad un altro. La Convenzione di Budapest ne è consapevole, e richiede che le richieste istruttorie siano soddisfatte "al più presto possibile quando" "vi è motivo di ritenere che i dati relativi siano particolarmente a rischio di perdita o modificazioni" (art. 31 § 3), obbligando al contempo gli Stati a predisporre un "punto di contatto" fra le autorità "disponibile 24 ore su 24 e 7 giorni su 7" (art. 35). È possibile, poi, che le autorità interessate riducano i tempi attraverso appositi accordi informali. Rimane alto, nondimeno, il pericolo che la trasmissione delle prove non avvenga in tempo utile per una proficua fruizione delle prove da parte dello Stato di emissione.

Un altro limite è dovuto al fatto che, per funzionare al meglio, la rogatoria e l'OEI presuppongono la possibilità di individuare un unico Stato di esecuzione e, di conseguenza, una sola *lex loci*. È ricorrente, negli atti normativi che li disciplinano, la clausola secondo cui l'autorità di esecuzione deve attenersi alle "formalità" e alle "procedure" espressamente indicate dall'autorità di emissione sulla base della *lex fori*, salvo che queste ultime confliggano con i "principi fondamentali" della *lex loci*, o portino

[5] Le rogatorie sono disciplinate, in particolare, dalla Convenzione del Consiglio d'Europa di assistenza giudiziaria in materia penale del 1959, recepita dall'Italia con la l. 23 febbraio 1961, n. 215, nonché, nel contesto dell'Unione Europea, dalla Convenzione di assistenza giudiziaria in materia penale del 2000, recepita con il d.lgs. 5 aprile 2017, n. 52. Per quanto riguarda l'uso della rogatoria per la raccolta transnazionale delle prove digitali, poi, va menzionata la Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001 (c.d. Convenzione di Budapest) L'OEI, dal canto suo, è disciplinato dalla direttiva 2014/41, recepita con il d.lgs. 21 giugno 2017, n. 108. Tutte queste prescrizioni sono integrate a livello nazionale, laddove non dispongano diversamente, dalle norme previste dagli artt. 723 s. c.p.p.

ad un'eccessiva compressione dei diritti fondamentali delle persone coinvolte[6]. Tale condizione – non esente da margini di ambiguità – se non altro mira ad evitare che le modalità di raccolta delle prove si appiattiscano su una *lex fori* non sufficientemente attenta alle garanzie, dando spazio ai superiori *standard* di tutela eventualmente previsti dalla *lex loci*, in una logica di contemperamento della sovranità dello Stato richiedente con quella dello Stato di esecuzione.

Ebbene, la dispersione delle prove digitali spesso porta alla moltiplicazione delle *lex loci*. Come identificare, in tali ipotesi, lo Stato di esecuzione? Dovrebbe essere lo Stato in cui opera o ha la sede legale il *service provider* che ha accesso alle prove? Oppure dovrebbe essere lo Stato in cui si trova il *server* dove le prove sono reperibili, magari diverso dallo Stato del *provider* [7]? E in quest'ultimo caso, come effettuare la scelta qualora, come spesso accade per ragioni economiche od organizzative, le prove vengano fatte costantemente circolare fra *server* situati in Stati diversi (c.d. *load balancing*) [8]?

A queste condizioni, è evidente come i vigenti strumenti di cooperazione giudiziaria diventino obsoleti. A fronte di una molteplicità di Stati a cui sarebbe possibile rivolgere la richiesta istruttoria, nessuno Stato, da solo, potrebbe fondatamente rivendicare il ruolo di Stato di esecuzione. Di qui il pericolo che quest'ultimo venga individuato in modo arbitrario o, comunque, sulla base di criteri incapaci di fornire una tutela adeguata delle garanzie: uno per tutti, il *forum shopping*, che consentirebbe all'autorità dello Stato di emissione di prescegliere lo Stato dotato del sistema di maggiori capacità repressive, e quindi più propenso a trasmettere le prove.

---

[6] Si vedano, per le rogatorie, gli artt. 4 della Convenzione del 2000 e 8 d.lgs. n. 52 del 2017, nonché, per l'OEI, gli artt. 9 § 2 direttiva 2014/41 e 4 comma 2 e 5 comma 3 d.lgs. n. 108 del 2017. Cfr. anche l'art. 27 § 3 della Convenzione di Budapest.

[7] Come accaduto, ad esempio, nel noto caso *Microsoft Ireland*, in cui un'autorità giudiziaria statunitense aveva chiesto alla Microsoft, azienda statunitense, alcuni dati reperibili in un *server* situato in Irlanda.

[8] Su queste variabili v. J. Daskal, *Borders and bits*, in *71 Vanderbilt Law review*, 2018, p. 190; S. Signorato, *Le indagini digitali*, cit., p. 199 s.; F. Siracusano, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Proc. pen. giust.*, f. 1, 2017, p. 180 ss.

3. Il nuovo paradigma della cooperazione diretta con i *service provider*

Visti i limiti della cooperazione fra organi statali, non stupisce che, nella prassi, abbia preso piede un metodo alternativo: la richiesta diretta da parte dell'autorità giudiziaria interessata alle prove ai *service provider* che le detengono, senza coinvolgere nessun altro Stato.

È un metodo che, allo stato, non trova una specifica regolamentazione. Non appare consentito rinvenirne un embrione operativo nell'art. 234 *bis* c.p.p., che ha trasposto nel nostro sistema l'art. 32 della Convenzione di Budapest. È vero che tale disposizione prescrive, laconicamente, che è "sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare". Quest'ultimo, tuttavia, non potrebbe essere identificato con chi, come un *service provider*, detenga dati altrui[9]; diversamente, si introdurrebbe la possibilità di ottenere i dati aggirando le vigenti norme sulla cooperazione. Né va trascurato che quello del consenso è, per intuibili ragioni, comunque un requisito difficile da soddisfare[10].

Non essendo regolata, la cooperazione diretta con i *provider*, attualmente, si fonda sulla *voluntary disclosure*: ciascuna azienda decide di volta in volta, sulla base dei propri interessi, se ed entro quali limiti collaborare. Il che spiega perché l'Unione Europea, ora, vorrebbe disciplinarla; un intento che si è concretizzato in una proposta tuttora in fase di gestazione[11], volta ad introdurre strumenti istruttori che, veicolati da un regolamento anziché da una direttiva, non avrebbero bisogno di

---

[9] Cfr. D. Negri, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Arch. pen.*, f. 3, 2015, p. 53.

[10] V. J. Spoenle, *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, in *coe.it*., 31 agosto 2010, p. 7.

[11] "*Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*" del 17 aprile 2018 (COM(2018) 225 final). In merito ad alcune possibili modifiche della proposta, v. R. Pezzuto, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, in *penalecontemporaneo.it*, f. 1, 2019, p. 67 s.

un'implementazione nazionale, ma sarebbero direttamente operanti nei singoli Stati, evitando di trovare declinazioni diverse nei vari sistemi[12].

Sullo sfondo di un intervento del genere vi è un cambio di paradigma della filosofia della cooperazione giudiziaria di non poco conto. I nuovi congegni non sostituirebbero, ma si affiancherebbero alla rogatoria e all'OEI, ampliando così le possibilità per le autorità giudiziarie dell'Unione di venire in possesso delle prove digitali non disponibili nei propri paesi[13]. Non è difficile prevedere, tuttavia, che, grazie alla loro maggiore efficacia applicativa, essi assumerebbero un'importanza preminente. È fondamentale, dunque, prendere coscienza dei limiti che li contraddistinguono.

4. La proposta di regolamento UE sull'ordine europeo di produzione e di conservazione delle prove digitali

In sintesi, la nuova modalità di cooperazione delineata dalla proposta di regolamento si basa sui seguenti capisaldi.

i) Vengono disciplinate due tipologie di richieste: l'ordine di produzione, mirato alla trasmissione dei dati; l'ordine di conservazione, finalizzato invece alla custodia dei dati in vista di una successiva richiesta di produzione, impedendone temporaneamente la cancellazione o la modifica.

ii) Gli ordini possono essere rivolti dalle competenti autorità nazionali direttamente ai rappresentanti legali dei *provider* che offrono i loro servizi nell'Unione Europea. Questi ultimi possono ricomprendere i

---

[12] Cfr. M. Gialuz-J. Della Torre, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *penalecontemporaneo.it*, f. 5, 2018, p. 292.

[13] Gli ordini di produzione e di conservazione non potrebbero, peraltro, essere utilizzati per effettuare intercettazioni, le quali continuerebbero a richiedere l'emissione di una rogatoria o di un OEI. Una restrizione comprensibile, in quanto dovuta all'esigenza di evitare di trasformarli in strumenti di prevenzione o, peggio, di sorveglianza occulta, nonché di addossare un (economicamente gravoso) dovere di monitoraggio continuo a carico dei *provider*: v. O. Pollicino-M. Bassini, *La proposta di Regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, in *medialaws.ue*, 26 ottobre 2018, p. 15.

fornitori sia di servizi di comunicazione elettronica (*email*), sia di servizi della c.d. società dell'informazione (come i *social network* o i prestatori di servizi di *hosting*), o di nomi di dominio *internet* e di numerazione IP (art. 2 della proposta).

iii) Gli ordini possono avere ad oggetto due tipologie di dati: quelli relativi agli "abbonati" e agli "accessi" da un lato, e quelli relativi alle "operazioni" e al "contenuto" dall'altro.

iv) Sono previste diverse condizioni tanto per l'emissione quanto per l'esecuzione degli ordini (artt. 4-10).

v) Soddisfatte tali condizioni, gli ordini di produzione vanno eseguiti rispettando tempistiche serrate: dieci giorni o, in caso di urgenza, addirittura sei ore dalla loro ricezione (art. 9); la conservazione dei dati, dal canto suo, deve iniziare immediatamente, per durare di regola sessanta giorni (art. 10).

vi) Quando, pur ricorrendone le condizioni, gli ordini non vengano eseguiti entro i termini previsti, i *provider* possono essere sottoposti a sanzioni pecuniarie da parte degli Stati in cui essi hanno la loro sede legale (artt. 13 e 14).

vii) Ai titolari dei dati, a prescindere dal fatto che siano persone sottoposte ad un procedimento penale o terzi, deve essere assicurato un mezzo di impugnazione esperibile nello Stato di emissione al fine di contestare le legittimità degli ordini di produzione (art. 17).

Si vorrebbe, in tal modo, creare un canale di cooperazione rapida ed efficace con chi detiene i dati, eliminando le lungaggini che, inevitabilmente, deriverebbero dall'esigenza di coinvolgere un altro Stato nelle operazioni istruttorie. Peraltro, come emerge dall'art. 1 § 2[14], i compilatori della proposta sono consapevoli del fatto che si tratta di attività suscettibili di interferire con i diritti fondamentali degli individui. Basti menzionare, fra questi, il diritto al rispetto alla vita privata (artt. 8 CEDU e 7 Carta di Nizza) e la libertà di espressione dei titolari dei dati

[14] Ai sensi del quale "il presente regolamento non ha l'effetto di modificare l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dall'articolo 6 TUE, compresi i diritti di difesa delle persone sottoposte a procedimento penale, e lascia impregiudicati gli obblighi spettanti a tale riguardo alle autorità di contrasto o giudiziarie".

(artt. 11 Carta di Nizza), nonché la libertà di iniziativa economica (art. 16 Carta di Nizza) dei *provider*.

Ne discende l'esigenza di rispettare, in particolare, il requisito della "necessità in una società democratica", richiesto dall'art. 8 § 2 CEDU ai fini del rispetto del diritto alla riservatezza. Il che, stando alla consolidata interpretazione della Corte europea dei diritti dell'uomo[15] e della Corte di giustizia dell'Unione Europea[16], si traduce nella "proporzionalità" delle misure da adottare: una condizione che presuppone l'impiego di garanzie processuali "adeguate e sufficienti contro l'abuso e l'arbitrarietà"[17], tali da assicurare che la compressione del diritto risulti strettamente indispensabile e, allo stesso tempo, non ne intacchi il nucleo essenziale.

Nei sistemi nazionali, queste garanzie si identificano, a seconda dei casi, con l'autorizzazione (preventiva o, perlomeno, successiva) delle operazioni istruttore da parte di un organo giurisdizionale, l'attinenza del procedimento ad un reato di una certa gravità e la sussistenza di indizi di colpevolezza. Come ora vedremo è, tuttavia, dubbio che la proposta di regolamento riesca pienamente ad assicurarle.

4.1. I limiti della proposta: a) le garanzie a geometria variabile.

La peculiarità della proposta consiste nell'adozione di un approccio a "geometria variabile", mirato a dosare le garanzie processuali in base alla tipologia di ordine da emettere e alle caratteristiche dei dati di interesse dell'autorità di emissione.

In generale tutti gli ordini, qualunque sia il loro contenuto, devono essere "necessari" e "proporzionati" (artt. 5 § 2 e 6 § 2). Questi due requisiti, di per sé piuttosto generici[18], assumono contorni più precisi se li si identifica con le condizioni di emissione dei corrispondenti atti istruttori che, in base alla *lex fori*, opererebbero a livello nazionale. Nel nostro

---

[15] V., fra le molte, Corte eur. dir. uomo, GC., 4 dicembre 2015, *Roman Zakharov c. Russia*, § 227 s.; Id., GC, 4 maggio 2000, *Rotaru c. Romania*, § 47 s.

[16] Cfr. Corte giustizia U.E., 8 aprile 2014, *Digital Rights Ireland*, C-293/12 e C-594/12, § 38 s.

[17] Corte eur. dir. uomo, 27 settembre 2018, *Brazzi c. Italia*, § 41.

[18] V. M. Gialuz-J. Della Torre, *Lotta alla criminalità*, cit., p. 293.

sistema, viene in gioco il presupposto di emissione delle perquisizioni informatiche (art. 247 comma 1 *bis* c.p.p.), ossia il "fondato motivo" di ritenere che dati "pertinenti al reato" oggetto del procedimento siano rinvenibili in un determinato spazio informatico o siano detenuti da un certo *service provider*.

Gli ordini di produzione, inoltre, possono essere emessi solo se "una misura dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello stato di emissione" (artt. 5 § 2). Il che significa che la legge deve contemplare la possibilità per gli organi inquirenti di svolgere indagini informatiche al fine di acquisire prove digitali detenute dai *provider*: una facoltà, in Italia, disciplinata dall'art. 254 *bis* c.p.p.

Ciò detto, se gli ordini meno problematici dal punto di vista del rispetto della *privacy* – ossia gli ordini di conservazione e gli ordini di produzione dei soli dati relativi agli abbonati o agli accessi – possono essere disposti in rapporto a qualsiasi reato (artt. 6 § 2 e 5 § 3), per gli ordini di produzione dei dati relativi alle operazioni e al contenuto – in linea di massima, ben più invasivi – è necessario che il procedimento abbia ad oggetto un reato punibile nello Stato di emissione con una pena detentiva di almeno tre anni, oppure uno dei gravi reati appositamente elencati dalla proposta (art. 5 § 4).

Il limite edittale dei tre anni, piuttosto basso, consente di ricomprendere la maggioranza delle fattispecie penali[19], nella sostanza annullando sotto questo profilo ogni differenza fra gli ordini più invasivi e quelli meno invasivi. Ma non è, tutto sommato, un difetto grave, se si pensa al fatto che, a livello interno, le indagini informatiche possono essere svolte in rapporto a qualsiasi tipo di reato.

Appare comprensibile, inoltre, la scelta di rinunciare al tradizionale requisito della doppia incriminazione. Ad esso deroga già la disciplina sull'ordine europeo di indagine penale, la quale consente la raccolta delle prove all'estero in rapporto a tutti i reati appositamente elencati in una lista (artt. 11 § 1 lett. *g* della direttiva 2014/41 e 11 d.lgs. n. 108/2017): illeciti che, punibili nello Stato di emissione con una pena di almeno tre anni di detenzione, sono considerati di gravità tale da giustificare per definizione

[19] Cfr. L. Bartoli, *Digital evidence*, cit., p. 105.

le operazioni istruttorie. Soprattutto, il più sopra menzionato fenomeno di possibile moltiplicazione della *lex loci* determinato dalla dispersione delle prove digitali rende la doppia incriminazione un criterio, spesso, inapplicabile, come tale da considerare superato.

Non appare censurabile neppure la possibilità per l'autorità di emissione di chiedere al *provider* di astenersi dall'"informare la persona i cui dati sono ricercati, per non ostacolare il pertinente procedimento penale" (art. 11 § 1 della proposta), ritardando l'informazione al momento in cui non vi sia più il rischio di compromettere le indagini[20]. Qualcosa del simile avviene già a livello nazionale, laddove vi è tutta una serie di atti "a sorpresa" che possono essere disposti dall'organo di accusa senza previamente informare il difensore (si pensi alle perquisizioni): una cautela indispensabile per evitare il rischio di pregiudicare l'efficace compimento dell'atto.

La proposta risulta, per converso, eccepibile nella misura in cui non assicura una piena attuazione del controllo giurisdizionale. Non va infatti dimenticato che, stando alla giurisprudenza della Corte europea dei diritti dell'uomo, la sottoposizione delle operazioni istruttorie invasive della *privacy* ad un vaglio – almeno successivo – di un organo indipendente rappresenta uno degli elementi del nocciolo duro del diritto[21]. Eppure la proposta introduce, a questo riguardo, tutta una serie di distinzioni. Un vaglio giurisdizionale preventivo è assicurato per i soli ordini di produzione dei dati relativi alle operazioni e al contenuto (art. 4 § 2). Per gli ordini di produzione dei dati relativi agli abbonati e agli accessi – che in prima battuta possono essere disposti anche solo da un pubblico ministero (art. 4 § 1) – ci si accontenta, invece, di un ricorso *ex post* "davanti ad un organo giurisdizionale dello Stato di emissione" in conformità alla *lex fori* (art.

---

[20] Per una critica v. invece, O. Pollicino-M. Bassini, *La proposta*, cit., p. 18.

[21] Lo ha ribadito, fra le più recenti, Corte eur. dir. uomo, 27 settembre 2018, *Brazzi c. Italia*, § 1 s. relativa ad una perquisizione di un'abitazione e dei *personal computer* ivi rinvenuti disposta da un pubblico ministero in un procedimento per evasione fiscale. La mancanza di un'autorizzazione preventiva di un giudice – non richiesta, a livello interno, dall'art. 247 c.p.p. – è stata giudicata dalla Corte europea incompatibile con l'art. 8 CEDU per la ragione che alla perquisizione non era seguito nessun sequestro, e dunque l'interessato non aveva potuto esperire il riesame ai sensi dell'art. 257 c.p.p. (in modo da attivare un vaglio giurisdizionale perlomeno posticipato).

17 § 3) [22]: una disparità di trattamento che, a ben guardare, non risulta giustificata, se si considera che gli ordini di produzione hanno ad oggetto categorie di dati per alcuni versi sovrapponibili[23]. Possono essere emessi da un pubblico ministero (art. 4 § 3) senza un controllo giurisdizionale nemmeno successivo, infine, gli ordini di conservazione, ed è una scelta difficilmente comprensibile. Per quanto questi ultimi non consentano la "divulgazione dei dati" [24], nondimeno pregiudicano la facoltà del titolare di modificarli ed usarli liberamente[25]. Il fatto che non siano in nessun modo impugnabili, oltretutto, determina un'evidente tensione con il diritto ad un ricorso effettivo previsto dall'art. 47 della Carta di Nizza[26].

4.2. b) La privatizzazione della tutela dei diritti fondamentali.

L'aspetto più preoccupante della proposta consiste nell'affidare ai *provider* – aziende private e non organi pubblici – il controllo sull'eseguibilità degli ordini.

Gli argomenti a sostegno di tale soluzione sono, essenzialmente, di tipo utilitaristico. Si osserva, in particolare, che i *provider* a cui gli ordini sono rivolti svolgono, sia pure virtualmente, un'attività economicamente redditizia nello Stato di emissione, nel quale hanno collocato la loro sede operativa magari per ragioni fiscali. Sarebbe la giurisdizione di quest'ultimo, pertanto, a venire principalmente in gioco ai fini dello svolgimento delle attività istruttorie. Né va dimenticato che la raccolta

---

[22] Il quale sia tale da includere "la possibilità di contestare la legittimità della misura, comprese la sua necessità e la sua proporzionalità".

[23] Si pensi, in particolare, ai dati sulle operazioni (ad esempio, come chiarisce l'art. 2 § 7 della proposta, la "fonte e il destinatario di un messaggio", o "altro tipo di interazione"), che potrebbero facilmente essere scambiati per dati sugli accessi (ossia quelli riguardanti "l'inizio o la fine di una sessione di accesso al servizio"), fruendo così del livello di garanzia inferiore; oppure ai dati relativi alla cronologia di ciascun utente o alle ricerche effettuate, in rapporto a cui sorgerebbero non pochi dubbi di collocazione e, quindi, sulle garanzie da applicare: V. O. Pollicino-M. Bassini, *La proposta*, cit., p. 14.

[24] Così la spiegazione dell'art. 17 della proposta.

[25] Cfr. M. Gialuz-J. Della Torre, *Lotta alla criminalità*, cit., p. 292.

[26] V. R.M. Geraci, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento di* e-evidence, in *Cass. pen*., 2019, p. 1360.

delle prove digitali tramite gli ordini di conservazione e di produzione non comporta nessun ingresso fisico da parte degli organi inquirenti dello Stato di emissione in un altro Stato, la cui sovranità non potrebbe, dunque, considerarsi realmente lesa[27].

Non è facile sostenere, tuttavia, che l'esclusione dai giochi degli organi pubblici dello Stato di esecuzione sia del tutto indolore. I criteri di controllo da impiegare ai fini dell'eseguibilità degli ordini di produzione e di conservazione sono, nella sostanza, non molto diversi da quelli utilizzabili dalle autorità giudiziarie chiamate ad eseguire le rogatorie e gli OEI. E se si considera che fra essi rileva la "manifesta violazione" della Carta di Nizza o la "manifesta arbitrarietà" (art. 14 commi 4 e 5 della proposta), è evidente come il vaglio del rispetto dei diritti fondamentali finisca per essere privatizzato.

Non si tratta, peraltro, di una peculiarità della proposta. Una prescrizione non dissimile si riscontra nel *CLOUD Act* del 2018, l'omologo statunitense del regolamento eurounitario, il quale prescrive che i *provider* potrebbero rifiutarsi di trasmettere i dati in presenza di un "rischio effettivo" di violazione del diritto di uno Stato straniero (§ 103[28]). Non dissimile il discorso per quanto concerne, più in generale, la tutela della *privacy* digitale a livello europeo; basti pensare al diritto alla deindicizzazione dei contenuti rinvenibili nei siti, anche esso sottoposto allo scrutinio delle aziende private che gestiscono i motori di ricerca[29].

Ci troviamo, dunque di fronte ad un *trend* che si sta imponendo a livello globale, e che proprio per questo deve essere considerato con la massima cautela. Vi è chi lo guarda con favore, notando come l'eliminazione del controllo da parte dei competenti organi dello Stato di esecuzione semplifichi non poco la procedura, con l'effetto di aumentare l'efficienza delle investigazioni. Inoltre i *service provider* – secondo questa impostazione – si troverebbero nella migliore posizione per effettuare il controllo, vuoi perché dotati delle specifiche competenze tecniche necessarie al riguardo, vuoi perché in possesso delle informazioni

---

[27] Cfr., al riguardo, P. de Hert-C. Parlar-J. Thumfart, *Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland*, in *New Journal of European Criminal Law*, vol. 9 (3), 2018, p. 338 s.

[28] La quale ha modificato la § 2713, tit. 18, cap. 121 dello *United States Code*.

[29] Cfr. O. Pollicino-M. Bassini, *La proposta*, cit., p. 10 s.

rilevanti. Si tratterebbe, del resto, di un vaglio fondato su indici giuridici "di agevole riconoscibilità anche per operatori privati", tali da non implicare necessariamente "l'esigenza di un apprezzamento di carattere tecnico" [30].

In caso di pericolo di violazione dei diritti – si conclude – comunque opererebbe un'ancora di salvataggio: la procedura di riesame prevista dall'art. 15 della proposta, attivabile quando il *provider* ritenga che l'ottemperanza di un ordine di produzione sia in contrasto con il diritto di un paese terzo che vieti la divulgazione dei dati "per la necessità di tutelare i diritti fondamentali delle persone interessate". In evenienze del genere, un organo giurisdizionale dello Stato di emissione dovrebbe riconsiderare la situazione e, se accertasse l'esistenza di una possibile violazione, dovrebbe interpellare il paese terzo, il quale potrebbe anche arrivare ad opporsi all'esecuzione dell'ordine. In questo modo, i *provider* diventerebbero "il perno centrale del sistema, fungendo da valvola in grado di regolare l'ingresso di un determinato ordine proveniente dall'autorità di emissione di uno Stato membro nell'ordinamento in cui i dati oggetto di ricerca sono materialmente conservati" [31].

Ci sono, tuttavia, forti dubbi che un tale complesso meccanismo possa sortire i suoi effetti, e ciò per una ragione connessa alla stessa essenza dei *provider*: i quali, a causa della loro natura privatistica e della conseguente – e legittima – esigenza di proteggere i loro interessi, non potrebbero mai agire come organi pubblici in posizione di imparzialità, di per sé del tutto indifferenti all'esito del vaglio[32]. Per quanto possano avere a cuore la tutela della *privacy* dei loro utenti, la loro condotta sarebbe condizionata dalla comprensibile necessità di mantenere buoni rapporti con gli Stati in cui esercitano la loro attività economica. Il

---

[30] O. Pollicino-M. Bassini, *La proposta*, cit., p. 17.

[31] O. Pollicino-M. Bassini, *La proposta*, cit., p. 11.

[32] Cfr. M. Böse, *An assessment of the Commission's proposals on electronic evidence*, in *europarl.europa.eu*, 21 settembre 2018, p. 41 s.; V. Mitsilegas, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in *Maastricht Journal of European and Comparative Law*, vol. 25 (3), 2018, p. 264 s. Si veda anche il *3rd working document* del Parlamento europeo sulla proposta di regolamento del 13 febbraio 2019, in *europarl.europa.eu*, p. 5 s., nonchè P. de Hert-C. Parlar-J. Thumfart, *Legal arguments*, cit., p. 351 s., secondo cui la proposta è più attenta alle esigenze repressive che alla tutela della sovranità degli Stati coinvolti e dei diritti degli individui.

rischio, poi, che, rifiutandosi di eseguire gli ordini di conservazione o produzione dei dati, siano esposti a sanzioni, inevitabilmente falserebbe le loro valutazioni. Non ci sarebbe da stupirsi, a queste condizioni, se svolgessero un vaglio superficiale, censurando solo le (probabilmente poche) istanze di acquisizione patentemente lesive dei diritti, in quanto prive di qualsiasi giustificazione (si pensi alle c.d. *fishing expeditions*, richieste "al buio" volte a sapere quali dati siano in mano ad un certa azienda). Un tendenziale lassismo a cui contribuirebbero i rapidi tempi di risposta imposti dalla proposta, nonché il fatto che, stando all'art. 8 commi 3 e 4 di quest'ultima, gli appositi certificati mediante cui gli ordini dovrebbero essere trasmessi ai *provider* non dovrebbero includere "i motivi della necessità e della proporzionalità della misura", ostacolando il controllo anche sotto questo profilo[33].

Così stando le cose, il rispetto dei diritti fondamentali sarebbe, alla resa dei conti, devoluto al solo Stato di emissione sulla base del proprio ordinamento, venendo meno qualsiasi forma di tutela delle legittime aspettative del titolare dei dati in merito all'applicazione della normativa di qualsiasi altro Stato coinvolto. Tale unica salvaguardia, però, potrebbe risultare inadeguata qualora la *lex fori* non fosse sufficientemente attenta alle esigenze garantistiche. Anche perché non va trascurato che l'art. 17 § 6 della proposta, riprendendo la medesima soluzione adottata dall'art. 14 § 7 della direttiva 2014/41 sull'ordine europeo di indagine penale, dispone che le violazioni del diritto di difesa e del diritto all'equo processo sono destinate a ripercuotersi solo sulla "valutazione" delle prove ottenute. Una prescrizione del genere non potrebbe che tradursi in una regola volta ad attribuire alle prove in questione un peso conoscitivo inferiore, magari tipo quella prevista, a livello interno, dall'art. 192 comma 3 c.p.p. in rapporto alle dichiarazioni dei coimputati[34]. Ma l'esperienza applicativa ha da tempo dimostrato come prescrizioni del genere siano poco efficaci, prestandosi a tutta una serie di elusioni consentite dall'elasticità della logica induttiva che governa l'accertamento dei fatti[35]. A fronte della

[33] Si veda il *3rd working document* del Parlamento europeo, p. 4.

[34] Le quali, viste dal nostro legislatore con sospetto, come noto devono essere assistite da specifici elementi di riscontro.

[35] Si rinvia a M. Daniele, *Regole di esclusione e regole di valutazione*, Giappichelli, 2009, p. 132 s.

lesione dei diritti fondamentali, la via più corretta sarebbe quella di decretare l'inutilizzabilità delle prove. Tale più radicale sanzione, però, è prevista come mera eventualità dal *considerando* 54 della proposta[36], non potendo dunque essere considerata una strada vincolata per i giudici nazionali chiamati ad applicare il regolamento.

5. L'esigenza di un approccio federalistico

Se la cooperazione fra organi pubblici risulta un passaggio ineludibile, ci si deve chiedere come rivitalizzarla, in modo da renderla compatibile con le caratteristiche delle prove digitali.

Nulla vieterebbe alla legge di individuare un unico Stato di esecuzione. Qui le soluzioni potrebbero essere molteplici. Lo si potrebbe identificare, ad esempio, con lo Stato in cui il *provider* ha la sede legale, oppure con lo Stato in cui si trova il *server* in cui sono ubicate le prove o, addirittura, con lo Stato indicato dallo stesso *provider*; in alternativa, ci si potrebbe riferire allo Stato di nazionalità del sospettato, o allo Stato di nazionalità della vittima[37]. A causa della dispersione delle prove digitali, tuttavia, qualunque scelta sarebbe arbitraria o, comunque, foriera di complicazioni, e quindi insoddisfacente.

Nello scenario "liquido" delle indagini informatiche, l'approccio meno problematico passa attraverso la creazione, in una logica federale, di un unico organo giurisdizionale europeo deputato a svolgere i controlli che la proposta vorrebbe affidare ai *provider*[38]. Un organo a cui le autorità giudiziarie nazionali dovrebbero rivolgere gli ordini di conservazione e di produzione, e a cui i *provider* che prestino i loro servizi nell'Unione dovrebbero trasmettere le informazioni rilevanti in loro possesso.

---

[36] Secondo cui la violazione dei diritti "può incidere sull'ammissibilità delle prove ottenute con detti mezzi o, a seconda del caso, sul peso di tali prove nell'ambito del procedimento".

[37] Per una rassegna, v. A.K. Woods, *Against Data Exceptionalism*, in *68 Stanford Law Review*, 2016, p. 764 s.

[38] In merito a questo tipo di soluzione, v. S. Carrera-G. González Fuster-E. Guild-V. Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*, Centre for European Policy Studies, 2015, p. 14 s.

Dovrebbe spettargli, in particolare, valutare se le richieste istruttorie rispettano gli *standard* di tutela dei diritti richiesti dalla CEDU e dalla Carta di Nizza; non potrebbe esimersi, a questo proposito, dal considerare la gravità dei reati oggetto del procedimento, le modalità e le circostanze di emissione del provvedimento, la presenza di elementi di prova a carico del sospettato già presenti in quel momento, nonché il contenuto e la finalità del provvedimento[39].

Non sarebbe, naturalmente, una soluzione priva di difetti. Dovrebbe essere un organo in grado di operare con la massima efficienza, capace di soddisfare in tempi ragionevolmente rapidi richieste provenienti da ogni parte del globo. A questo fine potrebbe forse essere utile prevedere, nei casi di urgenza, una procedura velocizzata: gli ordini che non apparissero manifestamente arbitrari potrebbero essere immediatamente eseguiti, per poi venire sottoposti ad un più approfondito vaglio successivo all'esecuzione, decretando *ex post* l'inutilizzabilità nello Stato di emissione dei dati raccolti qualora quest'ultimo avesse esito negativo[40]. In ogni caso, per quanto possa apparire difficile da realizzare, sarebbe una soluzione di gran lunga preferibile alla logica privatistica postulata dalla proposta di regolamento, suscettibile di aprire scenari dalle implicazioni davvero inquietanti per la tutela dei diritti.

Bibliografia

ATERNO, Stefano. Cloud forensics: aspetti giuridici e tecnici. In CADOPPI Alberto, CANESTRARI Stefano, MANNA Adelmo, PAPA Michele (a cura di). *Cybercrime*. Torino: Utet, 2019, p. 1689 s.

BARTOLI, Laura. Digital evidence for the criminal trial: limitless cloud and state boundaries. *Big data and Public Law: new challenges beyond data protection*, *rivista.eurojus.it*, 2019, num. spec., p. 96 s.

[39] Cfr. Corte eur. dir. uomo, 6 ottobre 2016, *K.S. e M.S. c. Germania*, § 44. V. anche Id., GC, 4 dicembre 2015, *Roman Zakharov*, cit., § 260, la quale richiede, ai fini delle intercettazioni, la presenza di un "ragionevole sospetto" a carico della persona sotto procedimento.

[40] Secondo un meccanismo non dissimile da quello adottato dall'art. 31 § 3 della direttiva sull'OEI in merito alle intercettazioni all'estero effettuate senza l'assistenza tecnica dello Stato straniero interessato.

BÖSE, Martin. *An assessment of the Commission's proposals on electronic evidence*. *europarl.europa.eu*, 21 settembre 2018.

CARRERA, Sergio, GONZÁLEZ FUSTER, Gloria, GUILD, Elspeth, MITSILEGAS, Valsamis. *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*, Brussels: Centre for European Policy Studies, 2015.

DANIELE, Marcello. La prova digitale nel processo penale. *Rivista di diritto processuale*. Padova, p. 283 s., 2011.

DANIELE, Marcello. *Regole di esclusione e regole di valutazione*, Torino: Giappichelli, 2009.

DASKAL, Jennifer. Borders and bits, *71 Vanderbilt Law Review*. p. 179 s., 2018.

DE HERT, Paul, PARLAR, Cihan, THUMFART, Johannes. Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland. *New Journal of European Criminal Law*, v. 9 (3), p. 326 s., 2018.

GERACI, Rosa Maria. La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento di e-evidence. *Cassazione penale*, p. 1340 s., 2019.

GIALUZ Mitja, DELLA TORRE Jacopo. Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali. *Penalecontemporaneo.it*, f. 5, p. 277 s., 2018.

MITSILEGAS, Valsamis. The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence, *Maastricht Journal of European and Comparative Law*, vol. 25 (3), p. 263 s., 2018.

NEGRI, Daniele. La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico). *Archivio penale*, f. 3, p. 44 s., 2015.

PEZZUTO, Raffaella. Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione. *Penalecontemporaneo.it*, f. 1, p. 57 s., 2019.

POLLICINO, Oreste, BASSINI, Marco. La proposta di Regolamento e-Evidence: osservazioni a caldo e possibili sviluppi. *Medialaws.ue*, 26 ottobre 2018.

SIGNORATO, Silvia. *Le indagini digitali*. Profili strutturali di una metamorfosi investigativa. Torino: Giappichelli, 2018.

SIRACUSANO, Fabrizio. La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione, *Processo penale e giustizia*, f. 1, p. 178 s. 2017.

SPOENLE, Jan. Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? C*oe.it*, 31 agosto 2010.

WOODS, Andrew Keane. Against Data Exceptionalism. *68 Stanford Law Review*, p. 279 s., 2016.

Informações adicionais e declarações dos autores (*integridade científica*)

Declaração de conflito de interesses (conflict of interest declaration): o autor confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores.

Declaração de ineditismo e originalidade (declaration of originality): o autor assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 22/08/2019
- Controle preliminar e verificação de plagio: 1/09/2019
- Avaliação 1: 16/09/2019
- Avaliação 2: 27/09/2019
- Decisão editorial preliminar: 21/09/2019
- Retorno rodada de correções: 04/10/2019
- Decisão editorial final: 08/10/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editoras-associadas: 2 (CC e BC)
- Revisores: 2

COMO CITAR ESTE ARTIGO:

DANIELE, Marcello. L'acquisizione delle prove digitali dai *service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1277-1296, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.288

La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información

The protection of personal data in the register of massive information storage devices

Miren Josune Pérez Estrada[1]
Universidad del País Vasco – España
mirenjosune.perez@ehu.eus
http://orcid.org/0000-0001-7402-4863

Resumen: El objeto de este trabajo es poner de manifiesto los problemas que plantea la investigación criminal cuando se analizan instrumentos tecnológicos en la averiguación del delito. En concreto, se estudia cómo afecta al derecho fundamental a la protección de los datos personales la prueba que se ha obtenido, con motivo de la investigación criminal, mediante el análisis de los datos contenidos en los dispositivos de almacenamiento masivo de la información. Se analiza el tratamiento jurídico que se da a la protección de los datos personales como parte de lo que se ha venido a denominar por la jurisprudencia "protección del entorno virtual" y las consecuencias jurídicas que tiene en el proceso penal. En definitiva, se quiere advertir cuáles son los efectos que tiene en el proceso penal la prueba que se ha obtenido vulnerando el derecho fundamental a la protección de los datos personales.

Palabras clave: Protección de datos de carácter personal; entorno virtual; dispositivos de almacenamiento masivo de información; garantías procesales; prueba ilícita.

Abstract: *This paper studies the affection of the personal data in the criminal investigation of the evidences of the mass storage devices of the information.*

[1] Profesora Adjunta de Derecho Procesal (acreditada Agregada). Departamento de Derecho Público. Facultad de Derecho. Sección Bizkaia.

The protection that jurisprudence gives to the protection of personal data is studied as "protection of the virtual environment" and also the possible consequences that it has in the criminal process, at the moment in which the judge evaluates the evidence, if the personal data of the researched have been achieved by violating the fundamental right to the protection of personal data.

Keywords: *Protection of personal data; virtual environment; massive information storage devices; procedural guarantees; evidence obtained violating fundamental rights of the process.*

Introducción

La investigación tecnológica en la averiguación del delito es compleja pero se ha convertido, en la actualidad, en imprescindible en la instrucción de la mayoría de los delitos para la averiguación de los hechos y la autoría de los mismos. El uso de técnicas tradicionales de investigación cede ante los resultados que proporcionan las nuevas técnicas de investigación. Las evidencias electrónicas prevalecen en la información que se encuentra disponible o almacenada en dispositivos de almacenamiento y constituyen fuente de prueba para poder acreditar el hecho investigado. Los dispositivos de almacenamiento masivo constituyen

efectos del delito en sí mismos pero, además, será necesario acceder a la información que contienen para la averiguación de los hechos. Precisamente, es en este acceso que, por otra parte, es inevitable donde se produce una lesión o afectación del derecho fundamental a la protección de los datos personales, además de a otros derechos como la intimidad y al secreto de las comunicaciones. Lo relevante será comprobar si la limitación al derecho fundamental es de suficiente entidad como para verse afectada la prueba obtenida y, en su caso, las consecuencias que tenga en el proceso penal.

Cómo afecta al derecho fundamental a la protección de los datos personales la investigación del material informativo que contienen los dispositivos de almacenamiento masivo de la información es el objetivo del trabajo. Partiendo del hecho que los datos personales sólo se pueden proteger desde el ejercicio de la facultad de autodeterminación individual[2] el problema que acucia a este derecho es el propio desconocimiento del peligro que entraña el acceso por terceros a los datos personales que no afectan a la vida íntima de la persona. Esta consideración de los datos, al margen de la esfera íntima, hace que no se repare en su utilización y manipulación que, inevitablemente, conlleva el control de la vida personal del individuo. No obstante, este derecho tiene como límites la propia investigación de un hecho delictivo aunque es necesario que esta investigación se realice de la manera más respetuosa al derecho que protege los datos personales porque sólo así la prueba obtenida en la investigación de los hechos criminales podrá ser válida en el proceso penal. Estudiamos en este trabajo el tratamiento procesal que, en la actualidad, se otorga a la protección de los datos personales como parte de lo que se ha venido a denominar por la jurisprudencia "protección del entorno virtual". Se analiza la regulación jurisdiccional nacional con motivo de la modificación

[2] MURILLO DE LA CUEVA, Pablo Lucas. La Constitución y el derecho a la autodeterminación informativa. *Cuadernos de Derecho Público*. Madrid, n. 19 – 20, 2003, pp. 36 – 39, apuesta por el nombre de autodeterminación informativa (también se conoce a este derecho como habeas data, libertad informática o protección de los datos personales) acuñado por el Tribunal Constitucional Federal alemán, sentencia de 15 de diciembre de 1983 y que entiende que expresa la sustancia del derecho: "El control de uno mismo sobre la información personal que le afecta y sirve para proyectarlo frente a la informática o frente a cualquier tecnología" (p. 39).

efectuada por la Ley Orgánica 7/2015, de 21 de julio que añade, por el art. único 36, el Capítulo I bis, el art. 236 bis al decies, sobre la Protección de datos de carácter personal en el ámbito de la Administración de Justicia y se examina si resulta adecuada para proteger los datos personales que se obtienen en una investigación criminal o en la fase de la instrucción procesal. Finalmente, se concluye exponiendo las consecuencias que tienen en el proceso penal los datos personales del investigado obtenidos vulnerando este derecho fundamental, en concreto, las consecuencias que tiene en la valoración de la prueba de los datos personales de la persona investigada que se han obtenido vulnerando este derecho fundamental.

1. Configuración del derecho fundamental a la protección de los datos personales

El derecho fundamental a la protección de los datos de carácter personal es un derecho de los que se han venido a denominar "tercera generación" y está en íntima relación con la incidencia negativa de las Tecnologías de la Información y de las Comunicaciones (TIC) en el ejercicio de los derechos fundamentales[3]. La protección de los datos

[3] Autores como PÉREZ LUÑO, Antonio Enrique (autor imprescindible por ser el iniciador en España de los estudios sobre esta materia), Intimidad y protección de datos personales: del "habeas corpus" al "habeas data. In: GARCÍA SAN MIGUEL, Luis (coord.). *Estudios sobre el derecho a la intimidad*. Madrid: Tecnos, 1992, pp. 36 – 45, lo califican como la "tercera generación de derechos humanos". Se trata del "derecho a la paz, los derechos de los consumidores, el derecho a la calidad de vida, o la libertad informática". También del mismo autor *Del Habeas Corpus al Habeas Data*. Conferencia impartida en el XIV Curso de Informática y Derecho. Centro Regional de la UNED, Extremadura, 1990,, p. 154 – 155, sostiene que "...nos hallamos ante una tercera generación de derechos humanos complementadora de las fases anteriores, referidas a las libertades de signo individual y a los derechos económicos, sociales y culturales. De este modo, los derechos y libertades de la tercera generación se presentan como una respuesta al fenómeno de la denominada "contaminación de las libertades" (*liberties pollution*), término con el que algunos sectores de la teoría social anglosajona aluden a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías.

Disponible en http://egov.ufsc.br/portal/sites/default/files/6_16.pdf. Fecha acceso: 07de junio de 2018.

personales no se recoge expresamente en el art. 18.4 CE[4] pero sí se contiene en él y ello como protección contra las amenazas a la dignidad, identidad, libertad e intimidad de las personas[5]. Estamos ante un derecho que pone de manifiesto la necesaria protección de los datos personales frente al tratamiento automatizado de los mismos que afecta al control de "nuestras vidas y personalidad" [6]; por lo tanto, el acento lo debemos poner en el "control" ejercido como poder sobre la otra persona, como disposición o manejo de la vida de las demás personas a través de sus datos personales.[7]

---

4 El punto 4. del art. 18 establece: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

5 La protección de los datos personales es el principal aspecto de la tutela de los derechos de las personas frente al uso de la informática a la que se refiere el art. 18.8 de la Constitución. De esta manera lo manifiesta MURILLO DE LA CUEVA, Pablo Lucas. La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Jurídicos (Nueva época)*. Madrid, n. 104, 1999. Sobre la importancia de la protección de los datos frente al uso de la informática y autónomo de la protección del derecho a la intimidad, PIÑAR MAÑAS, José Luis. La protección de datos personales y ficheros automatizados. In: ROMEO CASABONA, Carlos María (coord.). *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales.* Granada: Comares, 2006, pp. 153-167.

6 La línea jurisprudencial pionera en la tutela fundamental de los datos personales la marca la Sentencia del TC 254/1993, de 20 de julio, (BOE núm. 197, de 18 de agosto de 1993). Su importancia radica en que abre una línea jurisprudencial que conduce, posteriormente, al reconocimiento de este derecho fundamental y la conexión que establece entre el Convenio nº 108, de 28 de enero de 1981, del Consejo de Europa, sobre el tratamiento automatizado de los datos de carácter personal y el propio art. 18.4 CE, en atención al propio art. 10.2 CE (" Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España."). Supera de esta manera la doctrina de la Sala tercera del TS que los trata únicamente de principios. Estas consideraciones aparecen ampliamente argumentadas por el autor MURILLO DE LA CUEVA, Pablo Lucas, La Constitución y el derecho a la autodeterminación informativa, op. cit., p. 31.

7 MURILLO DE LA CUEVA, Pablo Lucas, La Constitución y el derecho a la autodeterminación informativa, op. cit., p. 36. Pone el autor de manifiesto que "...el riesgo específico que implica la informática es el control sobre las vidas de los demás que permite la captación incontrolada de información

El desarrollo del art. 18.4 CE se realiza con la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)[8], derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal (LOPD) que vino a transponer la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. En la actualidad, con motivo de la aplicación directa desde el 25 de mayo de 2018 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), se ha elaborado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[9].

---

personal...". "Es decir, la recopilación y el tratamiento automatizado de datos sobre los más variados aspectos de nuestras actividades..., de nuestras vidas y de nuestra personalidad... Y todo ello con la particularidad de que el resultado de esas elaboraciones, en tanto que producto de un tratamiento de datos, puede que ni siquiera sea verdad".

8 Fruto, además, de la ratificación del Convenio núm. 108 del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (entró en vigor el 1 de octubre de 1985).

9 BOE núm. 294, de 6 de diciembre de 2018. Junto a dicha normativa destacan los siguientes instrumentos jurídicos: La Carta de Derechos Fundamentales de la Unión Europea recoge, en su art. 8, la protección de datos de carácter personal y el Tratado de Lisboa, Declaración nº 21, firmado el 12 de diciembre de 2007, dispone la posibilidad de establecer normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en el ámbito de la cooperación judicial y policial. Podemos ver en este tema a GUTIÉRREZ ZARZA, María Ángeles.-, Protección de Datos Personales en la Carta de Derechos Fundamentales de la Unión Europea y El Tratado de Funcionamiento de la Unión Europea. In: GUTIÉRREZ ZARZA, María Ángeles (coord.). *Nuevas Tecnologías, Protección de Datos Personales y Proceso Penal*. Madrid: La Ley, 2012.

En el ámbito jurisdiccional la protección de los datos personales se encuentra también regulada en la legislación orgánica, Ley Orgánica del Poder Judicial (LOPJ) en su última modificación efectuada por la Ley Orgánica 7/2015, de 21 de julio añade por el art. único 36 el Capítulo I bis, el art. 236 bis al decies, sobre la Protección de datos de carácter personal en el ámbito de la Administración de Justicia. Se ha superado la regulación anterior incompleta y obsoleta que venía establecida por el Reglamento 1/2005, de aspectos accesorios a las actuaciones judiciales, aprobado por Acuerdo de 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial y por la LOPJ, art. 230.5 LOPJ.

2. Límites del derecho fundamental a la protección de los datos personales

El derecho fundamental a la protección de los datos no es absoluto. La limitación de su ejercicio viene dada de forma genérica en el art. 10.1 CE cuando se residencia en el orden público y la paz social[10]. El TC señala como límite del derecho fundamental a la protección de los datos personales, entre otros, la averiguación, persecución y castigo del delito[11]. El resto de derechos fundamentales y bienes jurídicos protegidos constitucionalmente actúan también como límite al ejercicio del derecho fundamental, en atención a la necesidad, proporcionalidad y a que sea "respetuoso con el contenido esencial del derecho fundamental restringido"[12].

---

[10] Art. 10.1 CE: "La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social."

[11] Lo recuerda la STC 292/2000, en su FJ 9: "En cuanto a los límites de este derecho fundamental no estará de más recordar que la Constitución menciona en el art. 105 b) que la ley regulará el acceso a los archivos y registros administrativos "salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas" (en relación con el art. 8.1 y 18.1 y 4 CE) ..."

[12] De esta manera lo recoge el FJ 11 de la STC 292/2000: "...en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos

De manera más específica los límites al derecho a la autodeterminación informativa los encontramos entre los derechos que protege el art. 24 CE y que comprende: tutela judicial efectiva, derecho a un proceso con todas las garantías, derecho de defensa[13] y el derecho a la prueba. Por lo tanto, debemos entender que el derecho a la protección de los datos personales del investigado o encausado, ie., el poder de control, de disposición de sus datos personales que se traduce en la imposición a terceros determinados deberes de hacer: "el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos" cede o "presenta ciertas limitaciones" en el proceso penal con el fin de conseguir llevar a buen término una investigación penal[14]. De esta manera lo establece el art. 236 quáter LOPJ: "De conformidad con lo dispuesto en el artículo 11.2 de la Ley Orgánica 15/1999, de 13 de diciembre[15], no será necesario el consentimiento del interesado para que los Tribunales procedan al tratamiento de los datos en el ejercicio de la potestad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud del propio Tribunal, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba.

En el Espacio de Libertad, Seguridad y Justicia (ELSJ) de la Unión Europea los límites a este derecho fundamental vienen impuestos por la Directiva (UE) 2016/680 del Parlamento europeo y del consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que

---

fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución..."

13 Una dimensión más amplia de los límites al derecho fundamental a la protección de datos en el proceso penal lo encontramos en Autor, 2018.

14 STC 254/1993, de 20 de julio, FJ 7.

15 Se debe entender referida a la normativa actual LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

se deroga la Decisión Marco 2008/977/JAI del consejo. La Directiva establece las normas sobre protección de los datos personales de las personas físicas respecto del tratamiento que realicen las autoridades con motivos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. En los supuestos de delincuencia transnacional la cooperación, basada en el principio de reconocimiento mutuo, entre autoridades policiales y judiciales resultará crucial para el esclarecimiento del delito grave y así se garantiza, a través de la Directiva, el intercambio de datos personales por parte de estas autoridades.

3. La protección del derecho fundamental de los datos personales frente a los nuevos métodos de investigación tecnológica en el proceso penal

3.1. Aproximación normativa

La reforma de la Ley de Enjuiciamiento Criminal (LECr) por la LO 13/2015, de 5 de octubre, de modificación de la LECr para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica [16] supuso dar cobertura legal a las medidas de investigación tecnológica[17]. De esta manera, se regulan las diligencias de investigación de intervención de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos. Se trata de los Capítulos IV a X del Título VIII ("De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución") que se añade por el

[16] BOE núm. 239, de 6/10/2015.

[17] Anteriormente, no existía una regulación concreta de esta materia en la LECr. En los supuestos de acceso a la prueba electrónica se aplicaban por analogía preceptos de la LECr y la amplía doctrina jurisprudencial que si se había desarrollado en esta materia

arts. únicos13 a 19 de la Ley Orgánica 13/2015, de 5 de octubre, arts. 588 bis a 588 octies.

La nueva regulación pretende dotar de mayor eficacia al derecho procesal a la vez que se procura que se actúe con pleno respeto a las garantías del proceso, sobre todo, cuando se pueden afectar derechos fundamentales de la persona, reconocidos en el art. 18 LECr[18]. Y es que la regulación de estas diligencias de investigación había sido ampliamente demandada por la doctrina[19] y jurisprudencia; en ese sentido, la STC 145/2014 recuerda la necesidad de una habilitación legal en los supuestos de injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas.[20]

Con la reforma de la LECr se cumple con las obligaciones que resultan de la ratificación del Convenio de Budapest sobre Ciberdelincuencia, de 23 de noviembre de 2001[21], que se aplica a la obtención de pruebas electrónicas[22] y se ha dado cobertura legal a las medidas de investigación

---

[18] Véase la Exposición de Motivos, apartado IV.

[19] Sobre este tema, véase, entre otros, ETXEBERRIA GURIDI, José Francisco. *La protección de los datos de carácter personal en el ámbito de la investigación penal*. Madrid: Agencia de protección de Datos, Premio Protección de datos Personales, 1998, pp. 22; CASTILLEJO MANZANARES, Raquel. *Hacia un nuevo proceso penal*. Madrid: La Ley, 2010y; BANACLOCHE PALAO, Julio; ZARZALEJOS NIETO, Jesús. Las diligencias de investigación restrictivas de los derechos fundamentales. In: *Aspectos fundamentales del Derecho Procesal Penal*. Madrid: La Ley, 3ª ed., 2015.

[20] La Sala Segunda del TC en su sentencia 145/2014 (ECLI:ES:TC:2014:145), FJ 7.

[21] BOE núm. 226, de 17 de septiembre de 2010.

[22] Art. 14.2 c) Convenio de Budapest sobre Ciberdelincuencia. La prueba electrónica o en soporte electrónico la define SANCHÍS CRESPO, Carolina. La prueba en soporte electrónico. In: GAMERO CASADO, Eduardo y VALERO TORRIJOS, Julián, (coords.). (, *Las tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*. Navarra: Thomson Reuters-Aranzadi,, 2012, p. 713, como "aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal". Con carácter general, la prueba en el proceso penal cabe definirla como "la actividad procesal, de las partes (de demostración) y del juez (de verificación), por la que se pretende lograr el convencimiento psicológico del juzgador acerca de la verdad de los datos alegados al proceso". De esta manera, la describe . BARONA VILAR, Silvia.

tecnológica, siguiendo la jurisprudencia de la Sala de lo Penal del TS. Destacamos entre la numerosa doctrina jurisprudencial las siguientes sentencias del TS: STS 250/2017, de 5 de abril[23], sienta la doctrina general sobre los presupuestos necesarios para la autorización de la interceptación de las comunicaciones telefónicas y telemáticas, STS 272/2017, de 18 de abril[24], sobre la utilización de dispositivos técnicos de captación de la imagen con motivo de la nueva regulación de la LECr y STS 786/2015, de 4 de diciembre[25], sobre registro de dispositivos de almacenamiento masivo de información, en este caso acceso al contenido de ordenadores; importa resaltar en esta sentencia la doctrina jurisprudencial sobre el derecho al propio entorno virtual.[26].

En el art. 588 bis LECr[27]se contiene la regulación de las disposiciones comunes a las medidas de investigación tecnológica que marcan los principios rectores de la autorización judicial que se otorgue al efecto. Estos principios disponen que la misma habrá de ser dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. Además, en los arts. 588 ter a 588 quinquies se regulan la interceptación de las comunicaciones telefónicas y telemáticas (Capítulo V), Captación y grabación de comunicaciones orales mediante la utilización de dispositivos

La prueba (I). In: MONTERO AROCA, Juan; GÓMEZ COLOMER, Juan Luis; BARONA VILAR, Silvia; ESPARZA LEIBAR, Iñaki; ETXEBARRIA GURIDI, José Francisco. *Derecho Jurisdiccional III. Proceso Penal.* Valencia: Tirant lo Blanch, 2017, p. 38.

23 Roj: STS 1582/2017 - ECLI: ES:TS:2017:1582.

24 ROJ: STS 1594/2017 - ECLI:ES:TS:2017:1594.

25 ROJ: STS 5362/2015 - ECLI:ES:TS:2015:5362.

26 Así mismo, una recopilación de las sentencias más recientes de la Sala de lo Penal del TS que asientan la doctrina jurisprudencial de los medios de prueba tecnológicos la realizan VILLEGAS GARCÍA, María Ángeles y ENCINAR DEL POZO, Miguel Ángel. Validez de medios de prueba tecnológicos. *Diario La Ley*. Madrid, n. 9005, Sección dossier, 2017.

27 Dispone así el artículo 588 bis a. LECr: "1. Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

electrónicos (Capítulo VI) y Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (Capítulo VII).[28]

La utilización habitual de las nuevas tecnologías hace necesaria la obtención de prueba de tipo tecnológico que, si bien es cierto que contribuirá a incrementar la eficacia judicial en la persecución de los delitos en igual medida aumentará el riesgo de lesividad del derecho fundamental a la autodeterminación informativa de las personas investigadas. A pesar de la protección constitucional de este derecho fundamental contenido en el art. 18.4 no se ha aprovechado la reforma de la legislación procesal para haber realizado una protección específica del derecho a la protección de los datos personales que pudiera verse con afectado con motivo de la obtención de prueba tecnológica. La importancia de esta protección va a hacer necesario que se legisle en el futuro en el sentido de una protección

---

[28] Existen otro tipo de medidas distintas a las procesales para averiguación del delito y la persona del delincuente. Son medidas de tipo predelictual utilizadas por el Estado a través de los agentes de la autoridad con la finalidad de garantizar la seguridad general que también contienen datos personales y, por lo tanto, necesitadas de la protección que se otorga a los datos de carácter personal. Son medidas policiales como la utilización de videocámaras en lugares públicos regulados por LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos (BOE núm. 186, de 5 de agosto de 1997), conservación de datos personales provenientes de comunicaciones electrónicas dispuesto en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE núm. 251, de 19/10/2007) y la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (DOUE núm. 119, de 4 de mayo de 2016). Los ficheros policiales utilizados para el ejercicio de la actividad policial que incorporan una ingente cantidad de datos personales y, de especial relevancia, por el tipo de datos personales que se contienen son las bases de datos policiales sobre identificadores de ADN. Los ficheros policiales se rigen por la normativa general de protección de datos personales. Sobre el tratamiento jurídico de los datos de carácter personal en determinadas diligencias de investigación véase al autor ETXEBERRIA GURIDI, José Francisco. *La protección de los datos de carácter personal en el ámbito de la investigación penal*, op. cit., pp. 159 y ss. En los casos de delincuencia transfronteriza se deben tener en cuenta las bases de datos de las siguientes instituciones: EUROPOL, EUROJUST y OlAF.

específica de manera separada al resto de derechos fundamentales que se contienen en el art. 18 CE.

3.2. Los dispositivos de almacenamiento masivo de información

El registro de dispositivos de almacenamiento masivo de la información se aborda en los arts. 588 bis sexies a, b y c LECr[29] (Capítulo VIII del Título VIII, Libro II, "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución"). La regulación del registro de los dispositivos de almacenamiento masivo de información refuerza la seguridad jurídica que se necesitaba en la obtención de la prueba electrónica a través de esta diligencia de investigación[30]. Se sigue la doctrina del TS que se incorpora a la

[29] Artículo 588 sexies a. Necesidad de motivación individualizada. Artículo 588 sexies b. Acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado. Artículo 588 sexies c. Autorización judicial.

[30] La doctrina ponía así de relieve la necesidad de una autorización judicial expresa habilitante para poder llevar a cabo el registro de este tipo de dispositivos de almacenamiento masivo de la información. Véase entre otros, CASTILLEJO MANZANARES, Raquel, Medios Probatorios, *Hacia un nuevo proceso penal*, op. cit., "...el procedimiento adecuado en estos supuestos, esto es, cuando se trate de la inspección o recogida de dispositivos y soportes de almacenamiento masivo de datos, es que la autorización judicial debería contener expresamente su práctica y sobre qué soportes se ha de realizar". Sobre este tema podemos ver también DELGADO MARTÍN, Joaquín. La prueba electrónica en el proceso penal. *Diario La Ley,* Madrid, n. 8167, Sección Doctrina, 2013; GONZÁLEZ-CUÉLLAR SERRANO, Nicolás. Garantías constitucionales en la persecución penal en el entorno digital. In GONZÁLEZ-CUÉLLAR SERRANO, Nicolás (ccord.). *Derecho y justicia penal en el siglo XXI*: *liber amicorum en homenaje al profesor Antonio González-Cuéllar García*. Madrid: Colex,, 2006, pp. 887-916, pp. 887-916; ORTIZ PRADILLO, Juan Carlos. Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica. *El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar y probar el delito*. In: PÉREZ GIL, Julio (coord.). Madrid: La Ley, 2012, pp. 267-310; PÉREZ GIL, Julio y GONZÁLEZ LÓPEZ, Juan José. La incorporación de datos personales automatizados al proceso en la propuesta de Código Procesal Penal. *Diario La Ley. Madrid,* n. 8217, 2013; CABEZUDO RODRÍGUEZ, Nicolás. Algunas reflexiones acerca de la reglamentación de las nuevas medidas de investigación tecnológica en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal. In: JIMENO BULNES, Mar y PÉREZ GIL, Julio (coords.).

regulación; así, entre otras muchas, la sentencia del TS 785/2008, de 25 de noviembre, F. J. 4, recuerda la doctrina consolidada de la Sala[31] "...esta Sala Segunda SSTS 985/2009 de 13.12, 342/2013 de 17.4, 587/2014 de 18.7, tiene declarado que: El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Por lo tanto, la jurisprudencia argumentaba y en esa línea se legisla que los dispositivos de almacenamiento masivo son algo más que una pieza de convicción a aportar a los autos y que habrá que estar a su contenido, ie., se debe tener en cuenta, en lo que en este trabajo concierne, que contiene datos de carácter personal; y en atención a ello es necesario o bien, el consentimiento del titular o un título habilitante, resolución judicial en forma de Auto, que fije, expresamente, los términos y alcance de los dispositivos que deben ser registrados.

3.3 Protección del derecho al entorno virtual

La cantidad y la calidad de información que contienen los dispositivos de almacenamiento masivo hace que resulten implicados diferentes derechos fundamentales. Estos dispositivos pueden contener información, datos sobre la vida personal y profesional de su titular pero, además, conversaciones o comunicaciones con otras personas. Así, estarían afectados el derecho a la intimidad o a la vida privada

Nuevos horizontes del derecho procesal: libro-homenaje al Prof. Ernesto Pedraz Peñalva. Barcelona: Bosch, 2016 . P. 541-558.

31 Roj: STS 7179/2008 - ECLI: ES:TS:2008:7179.

y el derecho al secreto de las comunicaciones junto con el derecho a la protección de los datos personales. El TC ha intentado describir el contenido de cada derecho fundamental atendiendo a los datos individualmente considerados[32] pero esta tarea cede ante el cúmulo de datos contenidos en los dispositivos de almacenamiento que hace que resulte imposible identificar de manera aislada los derechos fundamentales implicados, pues, muchas veces, aparecen entremezclados. El tratamiento individualizado de los datos personales que contienen los dispositivos de almacenamiento de información provoca cierta inseguridad jurídica al no existir una línea jurisprudencial uniforme sobre el contenido y límites del derecho fundamental afectado. Es más, incluso los datos personales tomados en cuenta de manera individualizada o aislada podrían resultar irrelevantes para su tutela jurisdiccional pero su tratamiento conjunto les otorga la necesidad de especial protección al resultar afectada la propia personalidad individual[33].

Se habla entonces del "derecho a la protección del propio entorno virtual". Ya desde la sentencia del TS 342/2013, de 17 de abril, F. J. 8, se pone de manifiesto esta circunstancia y la necesidad de autorización judicial habilitante que justifique el sacrificio del titular del dispositivo a

---

[32] El TC ha ido señalando, de manera casuística, los datos referidos a la vida íntima de la persona individualmente considerados, afirmando que "...el derecho a la intimidad comprende la información relativa a la salud física y psíquica de las personas, quedando afectado en aquellos casos en los que sin consentimiento del paciente se accede a datos relativos a su salud o a informes relativos a la misma" (SSTC 70/2009, Sala 1ª, de 23/03/2009, y 159/2009, Sala 2ª, de 29/06/2009), así como los datos económicos contenidos en el Impuesto de la Renta sobre las Personas Físicas (IRPF) en, entre otras, STC 233/1999, Pleno, de 16/12/1999.

[33] Es significativa en este sentido la sentencia del TC 173/2011, de 7 de noviembre, último párrafo del FJ 3º, que explica la especial idiosincrasia de los datos personales y la forma en que deben tutelarse: "Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona."

la protección de sus datos personales[34]. La importancia de esta sentencia 342/2013 radica, además, en que recoge el tratamiento jurídico que el TS realiza del contenido almacenado en el dispositivo electrónico[35]. Se

[34] Roj: STS 2222/2013 - ECLI: ES:TS: 2013:2222. En el F. J. 8 de la STS 342/2013 se recoge: "El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar -de hecho, normalmente albergará- información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones.

En consecuencia, el acceso a los contenidos de cualquier ordenador por los agentes de policia, ha de contar con el presupuesto habilitante de una autorización judicial. Esta resolución ha de dispensar una protección al imputado frente al acto de injerencia de los poderes públicos. Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal."

[35] El F. J. 8 de la STS342/2013 dice así: "La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento

decanta por la protección de "derecho al propio entorno virtual" que lo define como "toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos". Se trata de contemplar "de forma unitaria" mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado". El TS considera que el tratamiento jurídico de forma unitaria puede ser más adecuado para su protección jurisdiccional y lo denomina "derecho al propio entorno virtual" que tiene un plus de protección superior en el momento de su sacrificio que el tratamiento constitucional individualizado cada uno de esos derechos contemplados en el art. 18 CE.

De esta manera, el TS en la significativa sentencia 489/2018, de 23 de octubre, avala la técnica legislativa empleada en la reforma operada por la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, que

constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital. Sea como fuere, lo cierto es que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías."

comprende de forma unitaria, otorgando el mismo tratamiento jurídico, a todos los datos contenidos en los sistemas de almacenamiento masivo de la información. Es, precisamente, el tratamiento que se haga de los datos el que puede fácilmente describir un perfil personal del titular que es necesario proteger[36]. En palabras de la mencionada sentencia TS 489/2018, F. J. 5: "Algunos precedentes alientan la aparición de un derecho... con cierta vocación de emanciparse para cobrar autonomía e identidad propias. Partiendo de la plurifuncionalidad de los datos que se almacenan en cualquier ordenador y otros dispositivos asimilables por su capacidad de acumular información vinculada a una persona (*smartphone*) se conviene en la necesidad de un tratamiento unitario a partir de la proclamación de un derecho al entorno digital. Sería un derecho de nueva generación que serviría para alumbrar y justificar distintos escalones de protección jurisdiccional (SSTS 342/2013, de 17 de abril; 587/2014, de 24 de febrero, y 587/2014, de 18 de julio).

De ahí que en nuestra renovada legislación procesal haya emergido en fechas recientes, como diligencia específica que reclama garantías singulares (diferentes al registro de un vehículo o una maleta, por ejemplo), el registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies a) LECrim y ss., introducidos por la LO 13/2015, de 5 de octubre)." "...el mandato va dirigido a las fuerzas policiales... Pero ayuda la referencia en cuanto que, en buena medida, tal legislación se limita a conferir formato normativo a ideas ya presentes y exigidas en jurisprudencia precedente." Por lo tanto, la valoración por el juez de la procedencia de la medida de investigación del registro de dispositivos de almacenamiento masivo de información (debemos entender incluidos los equipos o sistemas informáticos) no requerirá la necesidad de precisar el derecho fundamental concretamente vulnerado sino tendrá como objetivo la protección del entorno virtual[37]. Y sólo en

---

[36] DELGADO MARTÍN, Joaquín. Derechos Fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos. *Diario La Ley*. Madrid, n. 8202, 2013. P. 3.

[37] En este sentido se pronuncia la sentencia del TS 342/2013, 17 de abril de 2013, F.J. 8 A) cuando argumenta que "La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de

el examen posterior, a la hora de motivar la adopción de la medida se entrará en el análisis particular de los derechos controvertidos.[38]

3.4 Extensión y límites del registro de dispositivos de almacenamiento masivo de la información

La necesidad de autorización judicial para acceder al contenido de los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, que se incauten con independencia de un registro domiciliario se exige en el art. 588 sexies c. LECr[39]. Y el contenido de la resolución judicial que autorice la medida deberá ser el que se establece en el punto 3 del art. 588 bis c[40]. Además de los requisitos referidos al hecho punible, la identidad de los investigados y la duración de la medida, entre otros, este artículo contiene la extensión y los límites en los que

---

vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos.".

[38] De esta manera lo argumenta la Circular de la Fiscalía General del Estado 5/2019, sobre registro de dispositivos y equipos informáticos, p. 7. Disponible en: <https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_5-2019.pdf?idFile=2a2c765e-3a04-4656-87c0-8b56ef73d0b6 >. Acceso en: 22 de junio de 2019.

[39] Se trata de las disposiciones comunes a las medidas de investigación tecnológica que se recogen el el Capítulo IV del Título VIII LECr: interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

[40] Vemos el contenido expreso en el punto 3 del art. 588 bis c. LECr.

se tiene que desarrollar esta medida de investigación tecnológica. De esta manera, el Auto que acuerde la medida de investigación debe determinar la extensión de la medida de injerencia, especificando su alcance, así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a LECr[41]. Se trata de especificar en la resolución judicial los términos exactos del registro, ie., los instrumentos o dispositivos tecnológicos a investigar, si en el mismo registro se podrá hacer copias de los datos que contengan los dispositivos, las condiciones para proteger la integridad de los datos que se aprehendan y establecer las garantías necesarias en el caso de un posterior análisis pericial[42].

El alcance del registro debe venir referido a la clase información o datos a los que se podrá acceder a través de la habilitación judicial que se deberá detallar, sin que exista necesidad de precisar los soportes físicos o virtuales que los contengan y que se puedan localizar con motivo del registro habida cuenta de la imposibilidad de enumerar todos los sistemas que los puedan contener dada su diversidad, por lo que bastará que el mandamiento judicial realice una mención genérica. De esta manera, se puede concretar el registro de los dispositivos de almacenamiento masivo a los datos referidos a la persona investigada con irrelevancia de la pertenencia del mismo incluso cabe la posibilidad que se habilite a registrar los datos almacenados con independencia de su titularidad. Se puede también especificar el tipo de información a la que se puede acceder, ie., a la clase de datos a que se registrarán teniendo en cuenta la tipología de datos existentes [43]. La posibilidad de acotar con precisión la medida de investigación de los dispositivos

---

[41] Recordaremos que estos principios de idoneidad, excepcionalidad, necesidad y proporcionalidad son doctrina reiterada del TC y se incorporan a la LECr mediante su reforma por LO 13/2015Cr.

[42] Sobre los términos en los que se tiene que desarrollar el registro de estos aparatos podemos consultar FERNÁNDEZ-GALLARDO,Javier Ángel. Registro de dispositivos de almacenamiento masivo de la información.-, *Revista jurídica de la Universidad de Santiago de Compostela,* vol. 25, n. 2, 2016, pp. 40-41.

[43] Se posibilita, por tanto, un registro selectivo como indica CABEZUDO RODRÍGUEZ, Nicolás. Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. *I*

de almacenamiento masivo de información supondrá respetar los principios de excepcionalidad y necesidad que rigen este tipo de intervenciones pero no siempre y en todos los casos se estará en disposición de realizar un detalle tan preciso de la medida de investigación que se habilita realizar y, en este caso, habrá que valorar si se trata de una mera infracción procesal o si, por el contrario, se produce una situación de indefensión en el que se ha visto vulnerado el derecho de defensa[44] .

3.5. Acceso a los datos por la Policía Judicial y consentimiento del interesado

La posibilidad de acceso a los datos personales contenidos en dispositivos de almacenamiento masivo de la información sin autorización judicial es posible en dos supuestos: se trata de los casos de urgencia o en el caso de consentimiento del interesado. Son supuestos en los que el monopolio jurisdiccional cede ante la necesidad de autorización judicial para acceder a los datos personales[45]. El primero de ellos, son actuaciones que lleve a cabo la Policía Judicial en los casos

Jornada del Boletín del Ministerio de Justicia: Las reformas del proceso penal" de 5 de noviembre de 2015.-, Madrid: Ministerio de Justicia, 2016, pp. 7-60

[44] Recordemos la jurisprudencia consolidada sobre la vulneración formal o la vulneración material de las normas procesales a los efectos que se pueda tutelar la existencia de una indefensión con relevancia constitucional: Sentencia TC 25/2011, de 14 de marzo (BOE núm. 86, de 11 de abril de 2011) ECLI:ES:TC:2011:25 y Sentencia TC 82/2002, de 22 de abril (BOE núm. 122, de 22 de mayo de 2002) ECLI:ES:TC:2002:82, entre muchas otras.

[45] FERNÁNDEZ-GALLARDO, Javier Ángel, Registro de dispositivos de almacenamiento masivo de la información, op. cit., pp. 48-51 recuerda que es doctrina consolidada del TC que la afectación de un derecho fundamental no es suficiente para justificar como presupuesto indispensable la previa autorización judicial salvo explícita habilitación legal; recuerda, por ejemplo, el registro de una maleta o de unos papeles que realiza la Policía sin necesidad de expresa autorización judicial. Así recoge: "La incidencia en la privacidad no lleva a cuestionar que pueda recibirse declaración a un testigo por la policía como medio de averiguación del delito, sin necesidad de previa autorización judicial motivada, ni de ningún otro requisito especial. Ni siquiera cuando ese interrogatorio, por exigencias de la investigación, conduce a adentrarse en reductos más sensibles de la privacidad"

de urgencia. Esta situación se regula por el apartado cuarto del art. 588 sexies c LECr en el que se recoge el supuesto de acceso directamente por la Policía Judicial a los datos que contenga el dispositivo incautado sin necesidad de autorización judicial previa. Se trata de los casos de urgencia en los que se aprecie un interés constitucional legítimo y que sea imprescindible la medida. En estos asuntos la Policía Judicial debe comunicar al Juez de manera inmediata y, en todo caso, en el plazo máximo de 24 horas, la actuación que se ha llevado a cabo para que el Juez competente, de forma motivada, revoque o confirme la actuación en un plazo máximo de 72 horas desde que la Policía Judicial ordenó la medida.

Esta posibilidad que ahora contempla la LECr estaba avalada por la doctrina constitucional; así, la sentencia TC 70/2002 reconoce, "La regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que sólo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad. De no existir ésta, los efectos intervenidos que puedan pertenecer al ámbito de lo íntimo han de ponerse a disposición judicial, para que sea el juez quien los examine. Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad."[46]Se establece el requisito temporal como motivo habilitante de la actuación judicial que supone que su transcurso puede perjudicar la investigación penal. En definitiva, se trata de proteger el interés general del Estado de persecución de los delitos por encima del derecho a la protección de los datos. Vemos aquí la aplicación de una dimensión de esa limitación del derecho fundamental a la protección de los datos personales que comentamos en epígrafe anterior.

[46] Se trata del FJ 9 de la Sentencia 70/2002, de 3 de abril (BOE núm. 99, de 25 de abril de 2002) ECLI:ES:TC:2002:70.

La siguiente exclusión, que señalábamos, a la necesidad de autorización judicial para el acceso a los datos contenidos en los dispositivos de almacenamiento masivo de la información es la referida a la prestación del consentimiento por el interesado. La exigencia del consentimiento únicamente se exige en el grado de tácito sin necesidad de que el titular del dispositivo debe realizar un consentimiento expreso. Si bien, la LECr guarda silencio sobre este aspecto del consentimiento pues no lo regula, el TC se ha pronunciado sobre el mismo en el aspecto indicado siendo relevante, entre otras la sentencia del TC 173/2011 que ampara el acceso a datos personales contenidos en dispositivos electrónicos a través de un consentimiento tácito del titular del mismo valorando también la extensión del consentimiento otorgado, ie., que la actuación invasiva de los datos no se haya extralimitado[47]. En cualquier caso, pese al esfuerzo del TC por amparar el consentimiento para el acceso de datos personales contenidos en los dispositivos de almacenamiento masivo se echa de menos en la tan reciente regulación de las medidas de investigación tecnológicas, recordemos por LO 13/2015, una regulación de las condiciones en las que se debe prestar ese consentimiento ya establecidas.

[47] La Sentencia 173/2011, de 7 de noviembre (BOE núm. 294, de 07 de diciembre de 2011). ECLI:ES:TC:2011:173 es clave en este tema que recoge el parecer del Alto Tribunal, así su FJ 2; "...hemos afirmado que el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (SSTC 83/2002, de 22 de abril, FJ 5 y 196/2006, de 3 de julio, FJ 5), aunque este consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29 de junio, FJ 3). Ahora bien, se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto "aun autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida" (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2). En lo relativo a la forma de prestación del consentimiento, hemos manifestado que éste no precisa ser expreso, admitiéndose también un consentimiento tácito. Así, en la STC 196/2004, de 15 de noviembre, en que se analizaba si un reconocimiento médico realizado a un trabajador había afectado a su intimidad personal, reconocimos no sólo la eficacia del consentimiento prestado verbalmente, sino además la del derivado de la realización de actos concluyentes que expresen dicha voluntad (FJ 9)".

Conclusiones: Efectos de la prueba obtenida mediante registro de dispositivos de almacenamiento masivo de la información vulnerando el derecho fundamental a la protección de los datos de carácter personal

Si partimos de la alta protección que se otorga a los datos de carácter personal como derecho fundamental hemos de llegar a la conclusión que la obtención de prueba vulnerando este derecho especialmente protegido debe tener unas consecuencias perjudiciales en su valoración. La más perjudicial sería la ilicitud de la prueba. A pesar de esta afirmación, no existe aún pronunciamiento jurisprudencial claro al respecto habida cuenta de que apenas hay alegaciones sobre la vulneración de ese derecho. Pero es que, además, en las pocas sentencias en que se trata la vulneración de los datos de carácter personal y su posible ilicitud a efectos probatorios se contempla de forma unitaria independientemente del formato en que se encuentren y se opta por una protección genérica: la protección del "derecho al entorno virtual o digital". Relevante en este tema es la sentencia del TS 287/2017 [48], que desestima el motivo de impugnación (F. J. 2, 2.1): "Mal puede hablarse, por tanto, de vulneración del derecho a la intimidad o al entorno virtual del acusado cuando los peritos no pudieron acceder a ningún contenido susceptible de ser protegido por su conexión con aquellos derechos. Bastaría, por tanto, subrayar que ningún dato privado del acusado llegó a incorporarse a la causa, a raíz del análisis del ordenador, para descartar la reivindicada alegación de prueba ilícita".

Tampoco reciben el mismo tratamiento jurisprudencial los datos de carácter personal que se han obtenido por un particular que los aprehendidos por la policía judicial con motivo de una investigación penal. Así, la sentencia del TS 116/2017, de 23 de febrero[49] que en el F. J. 6, distingue los dos supuestos: "...está fuera de discusión la necesidad

[48] Roj: STS 1487/2017 - ECLI: ES:TS:2017:1487. En este caso se desestima el motivo de impugnación (F. J. 2, 2.1): "Mal puede hablarse, por tanto, de vulneración del derecho a la intimidad o al entorno virtual del acusado cuando los peritos no pudieron acceder a ningún contenido susceptible de ser protegido por su conexión con aquellos derechos. Bastaría, por tanto, subrayar que ningún dato privado del acusado llegó a incorporarse a la causa, a raíz del análisis del ordenador, para descartar la reivindicada alegación de prueba ilícita."

[49] Roj: STS 471/2017 - ECLI: ES:TS:

de excluir el valor probatorio de aquellas diligencias que vulneren el mandato prohibitivo del art. 11 de la LOPJ. Pero más allá del fecundo debate dogmático acerca de lo que se ha llamado la eficacia horizontal de los derechos fundamentales, es evidente que la acción vulneradora del agente de la autoridad que personifica el interés del Estado en el castigo de las infracciones criminales nunca puede ser artificialmente equiparada a la acción del particular que, sin vinculación alguna con el ejercicio del ius puniendi, se hace con documentos que, más tarde, se convierten en fuentes de prueba que llegan a resultar, por una u otra circunstancia, determinantes para la formulación del juicio de autoría. El particular que por propia iniciativa desborda el marco jurídico que define la legitimidad del acceso a datos bancarios, ya actúe con el propósito de lograr un provecho económico, ya con el de fomentar el debate sobre los límites del secreto bancario, no lo hace en nombre del Estado. No rebasa el cuadro de garantías que define los límites constitucionales al acopio estatal de fuentes de pruebas incriminatorias. Nada tiene que ver esa actuación con la de un agente al servicio del Estado. Lo que proscribe el art. 11 de la LOPJ no es otra cosa que la obtención de pruebas (" no surtirán efecto las pruebas obtenidas...."). Es el desarrollo de la actividad probatoria en el marco de un proceso penal - entendido éste en su acepción más flexible- lo que queda afectado por la regla de exclusión cuando se erosiona el contenido material de derechos o libertades fundamentales". Del contenido de la sentencia se extrae que la consecuencia de la ilicitud de la prueba vulnerando un derecho fundamental, en este caso el de la protección de los datos personales, está dirigida a la actuación de los agentes de la autoridad para hacer efectivo el *ius puniendi* del Estado.

Incluso en alguna sentencia anterior, sentencia del TS 949/2006, de 4 de octubre de 2006[50] se concibe la vulneración del derecho a la autodeterminación informativa como conculcación de la normativa general de protección de datos de carácter general y no como ilicitud de la prueba por vulneración de derechos fundamentales en su obtención. En el F. J. 1 se recoge: "...si el almacenamiento de datos excesivos o innecesarios perjudica o contravine la normativa de la Ley de Protección

[50] Roj: STS 6190/2006 - ECLI: ES:TS:2006:6190.

de Datos será competencia de la Agencia de Protección de Datos investigar el fichero y reducirlo a los términos previstos por la Ley, pero todo ello para nada afecta a la identificación previa realizada con criterios adecuados. Es más, la Orden de 2.9.2003 del Departamento de Interior Vasco, limita su finalidad a las actividades de policía científica orientadas a relacionar personas con el espacio físico de la infracción penal. En atención a lo expuesto resulta que cualquier temor o recelo de un potencial ataque al "habeas data" está injustificado, sin que por otro lado tales temores tengan que ver con la vulneración del derecho fundamental a la intimidad de la recogida y custodia de muestras si tal cometido se ha realizado con plena acomodación a la normativa vigente. Lo que nunca puede excluirse -recuerda la sentencia citada 179/2006 de 14.2- es que cualquier persona pueda infringir la Ley, en cuyo caso estaría sujeto a las correspondientes sanciones penales o disciplinarias que fueran pertinentes. Pero esa eventualidad en nada afecta a la prueba practicada y a la recogida y conservación de las muestras genéticas, que en ningún aspecto atacan al derecho fundamental contemplado en el art. 18.1 CE.

En relación a la vulneración del art. 18.4 CE que consagra el derecho a la autodeterminación informativa, derecho que debe entenderse como aquel que ostenta toda persona física a la reserva y control de los datos que le conciernen en los distintos ámbitos de la vida, de tal suerte que pueda decidir en todo momento cuando, como y en qué medida esa información sea recogida, almacenada, tratada y en su caso transferida a terceros, así como a ser informado de los datos personales que a estos efectos se encuentren almacenados en ficheros o bases de datos, pudiendo acudir a los mismos con la posibilidad de exigir su identificación, puesta al día o cancelación . No obstante, este derecho como todos, tiene excepciones y puede ser limitado por razones de otro interés preponderante. En la Ley de Protección de datos se establece en el art. 6 la exigencia del consentimiento inequívoco del afectado, pero en el mismo precepto se establecen excepciones" (...) " Y en todo caso -insistimos- el hipotético incumplimiento del registro constituirá una irregularidad administrativa que en modo alguno supone la vulneración de un derecho fundamental que lleve aparejada la nulidad absoluta del análisis practicado".

Lo cierto es que no existe una distinción clara respecto a la normativa que es necesario aplicar en estos supuestos. Se ha superado la regulación incompleta y obsoleta que venía establecida por el Reglamento 1/2005, de aspectos accesorios a las actuaciones judiciales, aprobado por Acuerdo de 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial y por la LOPJ, art. 230.5 LOPJ por una más amplia y específica regulada en la legislación orgánica, mediante la LOPJ en su última modificación efectuada por la Ley Orgánica 7/2015, de 21 de julio añade por el art. único 36 el Capítulo I bis, el art. 236 bis al decies, sobre la Protección de datos de carácter personal en el ámbito de la Administración de Justicia. Pero se constata una deficiente cobertura legal en el ámbito jurisdiccional que, en ocasiones, se confunde con la normativa general de protección de los datos personales regulada por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales lo que ocasionará más de un problema en la práctica jurídica respecto a la normativa a aplicar. Se debería haber apostado por una regulación procesal específica dentro de la LECr y no en la legislación orgánica que regulara el tratamiento de los datos personales que se realiza en el ámbito jurisdiccional y los efectos que en el proceso penal provoca la obtención de la prueba vulnerando el derecho a la protección de los datos personales.

Conviene poner de manifiesto las consecuencias que en el proceso penal debe tener la obtención de manera ilícita de datos personales del investigado a los efectos de la valoración de la prueba así como, cuestionarse las consecuencias jurídicas del tratamiento ilegal de datos personales del imputado "obtenidos con motivo de una investigación penal anterior e incluidos en una base de datos para su utilización en otros procesos penales"[51]. Incluso, cuestionarse el tratamiento jurisdiccional que se otorga a los datos personales en "... el período que transcurre entre la obtención y la celebración del juicio

[51] Así lo cuestiona GUTIÉRREZ ZARZA, María Ángeles. La protección de datos personales como derecho fundamental del imputado, ¿también en el ámbito del proceso penal?. *La Ley penal*, Madrid, n. 71, 2010, p. 4 que entiende que la protección de los datos personales debe formar parte del conjunto de principios y derechos del proceso penal.

oral"[52]. Será necesario garantizar la integridad de los datos durante la tramitación del proceso penal[53].

Queda, aún, avanzar en el estudio de las consecuencias procesales que se derivan de la obtención de datos obtenidos de manera ilícita en los dispositivos de almacenamiento masivo que es la fuente de prueba que hemos analizado en este trabajo. Entiendo hubiera sido necesario que la reciente reforma de la legislación procesal penal realizase una protección específica del derecho a la protección de los datos personales afectado con motivo de la obtención de prueba tecnológica[54]. La importancia de los datos personales, que irá en aumento, se traducirá en otorgar mayores garantías procesales; lo cual hará necesario que se legisle en el sentido de una protección específica de manera separada al resto de derechos fundamentales que se contienen en el art. 18 CE. La normativa procesal

---

[52] ESPARZA LEIBAR, Iñaki. Protección de datos de carácter personal y proceso penal *El nuevo proceso penal sin código procesal penal*, celebrado en la Universidad de Santiago de Compostela, los días 9 y 10 de noviembre de 2017. In: ORDEÑANA GEZURAGA, Ixusko (coord.). *Justicia con ojos de mujer. Cuestiones procesales controvertidas.* Valencia: Tirant lo Blanch, 2018.

[53] DELGADO MARTÍN, Joaquín. Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015. *Diario La Ley,* Madrid, n. 8693, Sección doctrina, 2016, p. 3, destaca el problema de la manipulación de los datos: "...los datos pueden ser fácilmente modificados, sobre-escritos o borrados, lo que determina un peligro evidente de manipulación de las pruebas. De esta forma resulta necesario utilizar técnicas que permitan obtener dichos datos y garantizar su autenticidad e integridad durante la tramitación del proceso (cadena de custodia)." Las consecuencias en el proceso penal de los datos personales obtenidos violentando este derecho fundamental también lo pone de relieve FRÍAS MARTÍNEZ, Emilio. Protección y tratamiento de datos personales por el Ministerio Fiscal. *La Ley penal,* Madrid, n. 71, 2010. Protección de datos en el proceso penal, p. 7, quien no duda de la ilicitud de la prueba así obtenida: "Al elevar la protección de los datos de carácter personal a la categoría de derecho fundamental, la ilicitud en la obtención de los mismos tendrá consecuencias directas en la consideración de su valor probatorio, pues indudablemente los datos que hayan sido obtenidos con quebranto del derecho fundamental no podrán ser valorados para desvirtuar la presunción de inocencia".

[54] La doctrina procesal coincide en esta idea; así LÓPEZ-BARAJAS PEREA, Inmaculada. Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos, *Revista de Internet, Derecho y Política.* Madrid, n. 24, 2017, p. 73, p. 73, señala, también, alguna de las deficiencias normativas apuntadas.

deberá desarrollarse con mayor amplitud para dar mejor cobertura legal a los datos de carácter personal del investigado o encausado en el proceso penal.

No existe en este tema aún pronunciamiento jurisprudencial claro sobre las consecuencias de la valoración de la prueba vulnerando este derecho de protección de datos de carácter personal. No son muchas tampoco las alegaciones de parte sobre la ilicitud de la prueba con motivos de la vulneración de este derecho, quizá por esa falta de conciencia general sobre la protección de los datos personales a la que al principio del trabajo aludíamos. Pero es que, además, en las pocas sentencias en que se trata la vulneración de los datos de carácter personal y su posible ilicitud a efectos probatorios se contempla de manera conjunta junto con el resto de derechos fundamentales contenidos en el art. 18 CE y se opta por la protección del "derecho al entorno virtual o digital" al considerarlo con un plus de protección mayor que si se aprecian de manera individual . En cualquier caso, el acceso, a efectos probatorios, de los datos personales en el entorno virtual, que revelan el perfil personal del investigado, se ha de convertir en uno de los retos futuros que el legislador deberá plantearse proteger desde el ámbito de las garantías procesales[55].

Referencias bibliográficas

BANACLOCHE PALAO, Julio; ZARZALEJOS NIETO, Jesús. Las diligencias de investigación restrictivas de los derechos fundamentales. In: *Aspectos fundamentales del Derecho Procesal Penal*. Madrid: La Ley, 3ª ed., 2015.

BARONA VILAR, Silvia. La prueba (I). In: MONTERO AROCA, Juan; GÓMEZ COLOMER, Juan Luis; BARONA VILAR, Silvia; ESPARZA LEIBAR, Iñaki; ETXEBARRIA GURIDI, José Francisco. *Derecho Jurisdiccional III. Proceso Penal*. Valencia: Tirant lo Blanch, 2017.P. 38

[55] Recordemos, como arriba hemos apuntado, la falta de regulación en la LECr de las condiciones en las que el investigado debe prestar su consentimiento para poder acceder a su entorno virtual para que tenga validez en el proceso. Podemos ver un estudio de esta problemática realizado por FERNÁNDEZ-GALLARDO, Javier Ángel. El consentimiento del detenido al acceso a sus redes sociales y dispositivos de almacenamiento masivo de información. *La Ley Penal,* Madrid, n. 126, Sección Legislación aplicada a la práctica, 2017.

CABEZUDO RODRÍGUEZ, Nicolás. Algunas reflexiones acerca de la reglamentación de las nuevas medidas de investigación tecnológica en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal. In:JIMENO BULNES, Mar y PÉREZ GIL, Julio (coords.). *Nuevos horizontes del derecho procesal: libro-homenaje al Prof. Ernesto Pedraz Peñalva.)* Barcelona: Bosch, 2016 . P. 541-558.

CABEZUDO RODRÍGUEZ, Nicolás. Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. *I Jornada del Boletín del Ministerio de Justicia: Las reformas del proceso penal"* de 5 de noviembre de 2015.-, Madrid: Ministerio de Justicia, 2016. P. 7-60.

CASTILLEJO MANZANARES, Raquel.-, Hacia un nuevo proceso penal. Madrid: La Ley,, 2010.

CIRCULAR de la Fiscalía General del Estado 5/2019, sobre registro de dispositivos y equipos informáticos, p. 7. Disponible en: <https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_5-2019.pdf?idFile=2a2c765e-3a04-4656-87c0-8b56ef73d0b6>. Acceso en: 22 de junio de 2019.

DELGADO MARTÍN, Joaquín. Derechos Fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos. *Diario La Ley*.-Madrid, n. 8202, p. 3.

DELGADO MARTÍN, Joaquín. Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015. *Diario La Ley,* Madrid, n. 8693, Sección doctrina, 2016, p. 3.

DELGADO MARTÍN, Joaquín. La prueba electrónica en el proceso penal. *Diario La Ley,* Madrid, n. 8167, Sección Doctrina, 2013.

ESPARZA LEIBAR, Iñaki. Protección de datos de carácter personal y proceso penal *El nuevo proceso penal sin código procesal penal*, celebrado en la Universidad de Santiago de Compostela, los días 9 y 10 de noviembre de 2017. In: ORDEÑANA GEZURAGA, Ixusko (coord.). *Justicia con ojos de mujer. Cuestiones procesales controvertidas.* Valencia: Tirant lo Blanch, 2018.

ETXEBERRIA GURIDI, José Francisco. *La protección de los datos de carácter personal en el ámbito de la investigación penal.* Madrid: Agencia de protección de Datos, Premio Protección de datos Personales,, 1998, pp. 22 y 159 y ss.

FERNÁNDEZ-GALLARDO, Javier Ángel. El consentimiento del detenido al acceso a sus redes sociales y dispositivos de almacenamiento masivo de información. *La Ley Penal,* Madrid, n. 126, Sección Legislación aplicada a la práctica, 2017.

FERNÁNDEZ-GALLARDO,Javier Ángel. Registro de dispositivos de almacenamiento masivo de la información.-, *Revista jurídica de la Universidad de Santiago de Compostela,* vol. 25, n. 2, 2016, pp. 40-41.

FRÍAS MARTÍNEZ, Emilio. Protección y tratamiento de datos personales por el Ministerio Fiscal. *La Ley penal,* Madrid, n. 71, 2010. Protección de datos en el proceso penal, p. 7.

GONZÁLEZ-CUÉLLAR SERRANO, Nicolás. Garantías constitucionales en la persecución penal en el entorno digital.In GONZÁLEZ-CUÉLLAR SERRANO, Nicolás (ccord.). *Derecho y justicia penal en el siglo XXI*: *liber amicorum en homenaje al profesor Antonio González-Cuéllar García.* Madrid: Colex,, 2006, pp. 887-916.

GUTIÉRREZ ZARZA, María Ángeles. La protección de datos personales como derecho fundamental del imputado, ¿también en el ámbito del proceso penal?. *La Ley penal*, Madrid, n. 71, 2010, p. 4.

GUTIÉRREZ ZARZA, María Ángeles.-, Protección de Datos Personales en la Carta de Derechos Fundamentales de la Unión Europea y El Tratado de Funcionamiento de la Unión Europea. In: GUTIÉRREZ ZARZA, María Ángeles (coord.). *Nuevas Tecnologías, Protección de Datos Personales y Proceso Penal.* Madrid: La Ley,, 2012.

LÓPEZ-BARAJAS PEREA, Inmaculada. Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos, *Revista de Internet, Derecho y Política.* Madrid, n. 24, 2017, p. 73.

MARCOS AYJÓN, Miguel. Las múltiples implicaciones de la protección de datos en la justicia penal. In: GUTIÉRREZ ZARZA, María Ángeles(coord.). *Los avances del espacio de Libertad, Seguridad y Justicia de la UE en 2017: II Anuario ReDPE.*), Madrid: Wolters Kluwer, 2018.

MURILLO DE LA CUEVA, Pablo Lucas. La Constitución y el derecho a la autodeterminación informativa. *Cuadernos de Derecho Público.* Madrid, n. 19 – 20 2003), pp. 31, 36 – 39.

MURILLO DE LA CUEVA, Pablo Lucas. La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Jurídicos (Nueva época).* Madrid, n. 104, 1999.

ORTIZ PRADILLO, Juan Carlos. Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica. *El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar y probar el delito*. In: PÉREZ GIL, Julio (coord.). Madrid: La Ley, 2012, pp. 267-310.

PÉREZ ESTRADA, M. Josune. Efectos de la vulneración de la protección de los datos personales en el proceso penal. *La Ley Penal*, n. 35, Madrid, 2018.

PÉREZ GIL, Julio y GONZÁLEZ LÓPEZ, Juan José. La incorporación de datos personales automatizados al proceso en la propuesta de Código Procesal Penal. *Diario La Ley. Madrid,* n. 8217, 2013.

PÉREZ LUÑO, Antonio Enrique. *Del Habeas Corpus al Habeas Data*. Conferencia impartida en el XIV Curso de Informática y Derecho. Centro Regional de la UNED, Extremadura, 1990, p. 154 – 155.

Disponible en: <http://egov.ufsc.br/portal/sites/default/files/6_16.pdf>. Acceso en: 07de junio de 2018.

PÉREZ LUÑO, Antonio Enrique. Intimidad y protección de datos personales: del „habeas corpus" al „habeas data. In: GARCÍA SAN MIGUEL, Luis (coord.). *Estudios sobre el derecho a la intimidad*. Madrid: Tecnos, 1992, pp. 36 – 45.

PIÑAR MAÑAS, José Luis. La protección de datos personales y ficheros automatizados. In: ROMEO CASABONA, Carlos María (coord.). *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Granada: Comares, 2006, pp. 153-167.

SANCHÍS CRESPO, Carolina-., La prueba en soporte electrónico. In: GAMERO CASADO, Eduardo y VALERO TORRIJOS, Julián, (coords.). (, *Las tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*. Navarra: Thomson Reuters-Aranzadi,, 2012, p. 713.

VILLEGAS GARCÍA, María Ángeles y ENCINAR DEL POZO, Miguel Ángel. Validez de medios de prueba tecnológicos. *Diario La Ley*. Madrid, n. 9005, Sección dossier, 2017.

Informações adicionais e declarações dos autores
(integridade científica)

Agradecimentos (acknowledgement): Trabajo realizado en el contexto de las actividades que realiza el Grupo de investigación consolidado "Derechos Fundamentales y Unión Europea. Especial referencia al Espacio de Libertad, Seguridad y Justicia de la Unión Europea" (GIC IT-673-13, 2019-2021), financiado por el Gobierno Vasco.

Declaração de conflito de interesses (conflict of interest declaration): o autor confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

Declaração de ineditismo e originalidade (declaration of originality): o autor assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 05/07/2019
- Controle preliminar e verificação de plágio: 12/07/2019
- Avaliação 1: 23/07/2019
- Avaliação 2: 29/07/2019
- Decisão editorial preliminar: 23/08/2019
- Retorno rodada de correções: 08/09/2019
- Decisão editorial final: 20/09/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editora-associada: 1 (CC)
- Revisores: 2

COMO CITAR ESTE ARTIGO:

PÉREZ ESTRADA, Miren J. La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1297-1330, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.253

Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680[1]

Transfer and treatment of personal data in the criminal process. Progress and immediate challenges of the Directive (EU) 2016/680

Mª Isabel González Cano[2]

Universidad de Sevilla – España

maisabel@us.es

http://orcid.org/0000-0001-7856-8980

RESUMEN: La recogida u obtención, la cesión y el tratamiento de datos personales, en cuanto vía de investigación y obtención de material incriminatorio respecto al titular de tales datos, implican medidas que afectan a un derecho fundamental, el derecho a la protección de datos de carácter personal. Siendo ello así, la intromisión legítima de las autoridades competentes a los fines de represión, investigación y enjuiciamiento penal, deberá acomodarse a los estándares garantistas y a los principios rectores de toda medida de investigación que afecte a derechos fundamentales, tanto para legitimar tal medida como para la obtención de prueba de cargo o incriminatoria lícita. Así, la recogida, obtención y tratamiento de datos personales, a través de las medidas de investigación pertinentes, se deberá regir por los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de dichas medidas, a ponderar por la autoridad judicial que las autorice, con arreglo al art. 588 bis a. de la Ley de Enjuiciamiento Criminal.

[1] Este trabajo se ha elaborado en el marco de los siguientes Proyectos de investigación: Proyecto I+D+I de Excelencia DER2015-63942P (Ministerio de Economía y Competitividad), *"Instrumentos para el reconocimiento mutuo y ejecución de resoluciones penales: incorporación al Derecho español de los avances en cooperación judicial en la Unión Europea";* Generalitat Valenciana *"Claves de la justicia civil y penal en la sociedad del miedo"* –Prometeo 2018/2011-.

[2] (1.4.1965 - 20.10.2019) Era Catedrática de Derecho Procesal en la Universidad de Sevilla, España.

PALABRAS CLAVE: Cesión datos personales; proceso penal; prueba; principio de disponibilidad.

ABSTRACT: *Collection, transfer and processing of personal data, as a means of investigation and obtaining incriminating material regarding the owner of such data, involve measures that affect a fundamental right, the right to the protection of personal data. This being the case, the legitimate interference of the competent authorities for the purposes of repression, investigation and criminal prosecution, must conform to the guarantee standards and the guiding principles of any investigation measure that affects fundamental rights, both to legitimize such measure and to Obtaining evidence of legal charge or incrimination. Thus, the collection, collection and processing of personal data, through the relevant investigation measures, shall be governed by the principles of specialty, suitability, exceptionality, necessity and proportionality of said measures, to be weighed by the judicial authority authorizing them, in accordance with art. 588 bis a. of the Law of Criminal Procedure.*

KEYWORDS: *Transfer of personal data; criminal process; evidence; principle of availability.*

1. INTRODUCCIÓN. APROXIMACIÓN AL PRINCIPIO DE DISPONIBILIDAD DE LOS DATOS PERSONALES COMO INSTRUMENTO DE LA COOPERACIÓN JUDICIAL PENAL EN LA UNIÓN EUROPEA

En el desarrollo del Derecho europeo en materia de protección de datos personales, no se trata tan solo de regular el tratamiento de los datos personales desde una perspectiva general garantista, sino también desde el punto de vista de la cooperación judicial penal, y por tanto desde la perspectiva del llamado principio de disponibilidad de los datos personales, para facilitar la persecución, investigación y enjuiciamiento de fenómenos criminales transfronterizos[3].

Ciertamente, la vía general y garantista, es la primera que se desarrolla en el ámbito del Derecho Europeo, a través de la Directiva general de protección de datos personales de 1995, que conllevó la Ley española de protección de datos personales de 1999; la Directiva de 1997, sobre el tratamiento de los datos personales y la protección de la intimidad en las comunicaciones electrónicas, y la Directiva de 2002, en materia de telecomunicaciones, sobre las que volveremos más adelante.

Todas ellas son normas cuya finalidad esencial es la protección del titular de los datos personales, consagrando el control por el mismo, en orden a la necesidad de su consentimiento para la recogida, transmisión y procesamiento, y el derecho a la información, acceso, rectificación, cancelación y oposición. Sin embargo, hay otra vertiente del Derecho europeo sobre protección de datos que resulta imprescindible, la referida a la prevención, investigación y represión del delito, la vertiente especial y excepcional, que incide en la recogida de datos y su tratamiento en orden

---

[3] GONZÁLEZ CANO, *"Nuevos paradigmas de la cooperación judicial penal en la Unión Europea"*, en VVAA (ed. por BARONA VILAR), *Justicia civil y penal en la era global*, Tirant lo Blanch, Valencia, 2017, pp. 339 y ss. Sobre los orígenes de la protección de datos en Europa, v. VILLARINO MARZO, *"La Unión Europea ante los retos de la era digital. La reforma de la política europea de protección de datos",* en VVAA (dir. por PASCUA MATEO), *Derecho de la Unión Europea y Tratado de Lisboa,* Civitas, Madrid, 2013, pp. 561 a 565; GONZÁLEZ CANO, *"Algunas reflexiones sobre protección de datos personales, proceso penal y cooperación judicial penal en la Unión Europea",* en Cuadernos digitales de formación del Consejo General del Poder Judicial, Nº 29- 2012.

a la investigación y enjuiciamiento de la delincuencia, y en la que el titular de los derechos en materia de datos personales es a su vez sospechoso, investigado o encausado en un proceso penal.

Por tanto, la recogida u obtención, la cesión y el tratamiento de datos personales, en cuanto vía de investigación y obtención de material incriminatorio respecto al titular de tales datos, implican medidas que afectan a un derecho fundamental, el derecho a la protección de datos de carácter personal. Siendo ello así, la intromisión legítima de las autoridades competentes a los fines de represión, investigación y enjuiciamiento penal, deberá acomodarse a los estándares garantistas y a los principios rectores de toda medida de investigación que afecte a derechos fundamentales, tanto para legitimar tal medida como para la obtención de prueba de cargo o incriminatoria lícita.

Así pues, tales medidas pueden limitar el derecho a la protección de datos, concebido como un derecho fundamental autónomo respecto al derecho a la intimidad del art. 18.1 de la Constitución Española (en adelante, CE), en el sentido apuntado por el Tribunal Constitucional (en adelante, TC), así, en la STC 292/2000, de 30 de noviembre.

Por tanto, la recogida, obtención y tratamiento de datos personales, a través de las medidas de investigación pertinentes, deberá regirse por los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de dichas medidas, a ponderar por la autoridad judicial que las autorice, con arreglo al art. 588 bis a. de la Ley de Enjuiciamiento Criminal (en adelante, LECRIM).

Esta vertiente o perspectiva ligada a la investigación y obtención de fuentes de prueba, está conectada ineludiblemente a la cooperación policial y judicial penal en la Unión Europea (en adelante, UE), y por tanto a la lucha contra la criminalidad transfronteriza, que cuenta con importantes instrumentos y sistemas de investigación y tratamiento de datos personales, así como para el intercambio de datos sobre personas y objetos, tales como SIS (Sistema de información de Schenguen)[4], Europol,

[4] Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schenguen de segunda generación (SIS II) (DO L 205 de 7 de agosto de 2007, p. 63).

Eurojust, OLAF (Oficina europea de lucha contra el fraude), o el Sistema de información aduanero (SID)[5].

A raíz de los trágicos acontecimientos de 2001 en Nueva York, 2004 en Madrid o 2005 en Londres, se produce un punto de inflexión en la lucha contra las formas más graves de criminalidad. A partir de estos momentos, marcados por la llamada descentralización o globalización del fenómeno terrorista, comienza un intenso e imparable proceso en aras de la priorización de esa vía especial y excepcional sobre obtención, cesión y tratamiento de los datos personales, la vía represiva, representada por ejemplo por Eurojust, o por la Directiva de 2006 sobre conservación de datos en comunicaciones electrónicas, a la que nos referiremos más adelante.

La clave de este proceso se encuentra en el nuevo paradigma en la materia, que no es otro que el llamado principio de disponibilidad[6], con arreglo al cual, las autoridades competentes de los Estados de la UE tendrían acceso y podrían disponer de las informaciones en materia de investigación y enjuiciamiento penal, en las mismas condiciones con las que cuenta el Estado en el que la información está registrada[7].

---

[5] V. DREWER-GUTIERREZ ZARZA-MORÁN MARTINEZ, *"Intercambio de información y protección de datos personales en el ámbito de Eurojust, Europol y OLAF"*, en VVAA (coord.. por GUTIERREZ ZARZA*), Nuevas tecnologías, protección de datos personales y proceso penal,* La Ley, Madrid, 2012, pp. 129 y ss.

[6] Sobre la evolución de este principio en la cooperación policial y judicial, como elemento clave tanto en la inicial cooperación intergubernamental, como en los más recientes procesos de intercambio de información, FIODOROVA, *"La transmisión de información personal y datos personales en la Unión Europea para fines de investigación de delitos",* en VVAA (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, Pamplona, 2015, pp. 126 a 132; IDEM, "*Cesión de datos personales en posesión de Europol",* en VVAA (dir. por COLOMER HERNÁNDEZ), *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios,* Aranzadi, Pamplona, 2017, pp. 145 y ss.

[7] GALÁN MUÑOZ, "*La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea"*, en VVAA (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales..., op. cit,* pp. 42 y ss; IDEM, *"Los nuevos instrumentos de prevención y lucha contra el nuevo terrorismo: malas noticias para la intimidad y otros derechos fundamentales"*, en VVAA, *Cesión de datos personales y evidencias...,* op. cit., pp. 81 y ss.

El principio de disponibilidad supone, por una parte, la obligación de tener los datos disponibles y cederlos a estos fines, es decir, para la investigación y el enjuiciamiento penal (principio de finalidad); y, por otra, la posibilidad de que esta cesión de datos no venga regida con carácter general por el principio de especialidad, es decir, la posibilidad de que la autoridad del Estado cesionario los utilice para investigar o enjuiciar un delito diferente de los alegados para solicitar y justificar la cesión.

2. EL PRINCIPIO DE DISPONIBILIDAD EN LA DECISIÓN MARCO 2008/976/JAI, DE 27 DE NOVIEMBRE DE 2008

La más reciente evolución del principio de disponibilidad, su ámbito de aplicación, principios rectores y las garantías aplicables al interesado, pasa por varios hitos normativos. La circulación de datos personales a efectos de la persecución penal, ya se contempló en el Programa de Tampere, ya que las Conclusiones del Consejo Europeo de Tampere de octubre de 1999, confirmaron la necesidad de mejorar el intercambio de información entre las autoridades policiales de los países de la UE, y el Programa de La Haya de 2004 a 2009 la corroboró en noviembre de 2004. Por su parte, el Programa de La Haya de 2005 a 2010, específicamente recoge el citado principio de disponibilidad en todo el territorio de la Unión a efectos represivos, de tal manera que se hagan compatibles la protección de los derechos fundamentales y la seguridad al compartir la información (art.2.1).

Sin remontarnos a importantes instrumentos, como el Tratado de Prüm para la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, firmado el 27 de mayo de 2005[8],

[8] Estos sistemas de acceso se incorporaron en su momento a la Propuesta de la Comisión de DM del Consejo sobre intercambio de información en virtud del principio de disponibilidad (COM (2005) 490 final). Por otra parte, hay que tener presente que las primeras iniciativas en orden a la utilización de perfiles de ADN en la investigación y el enjuiciamiento criminal se remontan a la Resolución del Consejo 97/C 193/02, sobre intercambio de resultados de análisis de ADN, de la que parte la creación de bases de datos nacionales de

dos fueron los textos en los que este paradigma de la disponibilidad está más presente. Nos referimos a la Decisión 2008/615/JAI, del Consejo, de 23 de junio de 2008, sobre cooperación transfronteriza en materia de terrorismo y delincuencia organizada (llamada Decisión Prüm); y a la DM de 2006/960, obre simplificación en el intercambio e inteligencia de los Servicios de Seguridad [9].

Sin embargo, es la DM 2008/977/JAI, de 27 de noviembre de 2008, sobre protección de datos en el marco de la cooperación judicial en materia penal[10], la que consagra el paradigma de la disponibilidad en la transmisión de datos personales en causas penales, un paradigma ya contemplado como hemos visto en el Tratado de Prüm y en las Decisiones para su implementación.

A nuestro entender, la DM 2008/977 merece ser objeto de una doble valoración, la primera referente a sus logros, y la segunda a los motivos de su escaso éxito, del cual derivan las iniciativas que han conducido a la Directiva 2016/680, de la que nos ocuparemos a continuación.

En cuanto a la primera de las valoraciones propuestas, la DM de 2008 se refiere a la necesidad de establecer el marco de la protección

---

ADN para el intercambio automatizado de datos entre los Estados miembros. Igualmente, la Resoluciones del Consejo 2001/C-187/1, y 2009/C--296/1, sobre determinación de marcadores de ADN a utilizar en las analíticas y para facilitar el intercambio de resultados de las mismas.

9 Sobre los antecedentes y la estructura de la Decisión Prüm, DE HOYOS SANCHO, *"Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos"*, en VVAA (dir. por ARANGUENA FANEGO), *Espacio europeo de libertad, seguridad y justicia: últimos avances en cooperación judicial penal,* Lex Nova, Valladolid, 2010, pp. 152 y ss. Idénticas finalidades se persiguen en la más reciente Directiva 2017/541 relativa a la lucha contra el terrorismo, y que remplaza la Decisión Marco de 2002/2008 sobre la misma, VERVAELE, *"¿La asociación organizada terrorista y sus actos anticipativos: un derecho penal y política criminal sin límites?",* en VVAA (dir. por GONZALEZ CANO), *Integración europea y justicia penal,* Tirant lo Blanch, Colección Alternativas, Valencia, 2018, pp. 207 y ss. V, también, FREIXES SANJUAN, *"Protección de datos y globalización. La Convención de Prüm",* en Revista de Derecho Constitucional europeo, nº 7, enero – junio de 2007, p. 4.

10 DM 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO L 350 de 30 de diciembre de 2008, p. 60).

de datos en el ámbito de su cesión y tratamiento a efectos penales entre Estados, y de garantizar en cualquier caso la legalidad y la licitud en el tratamiento de dichos datos a intercambiar, y la exactitud de los datos, fundamental para su uso en una causa penal.

No debemos olvidar en este punto que, como veíamos en las páginas iniciales de este trabajo, con anterioridad a la DM 2008/977, el panorama normativo sobre esta materia, y también el plano institucional, la estructura orgánica de la cooperación judicial y el propio sistema de fuentes empleado, eran complejos y enrevesados. Por una parte, los primeros desarrollos del principio de reconocimiento mutuo, desde 2002 a 2010, no se centraron tanto en la aproximación normativa como en la armonización en cuanto a instrumentos de investigación y enjuiciamiento. Y, además, existen regulaciones que afectan a estas materias en Decisiones, Convenios o Reglamentos, sin contar con la normativa de las diversas agencias y organismos europeos que de forma más o menos directa se ocupan de la protección de datos y también de su cesión y tratamiento a efectos policiales y judiciales, como es el caso de Eurojust o Europol, o los ya citados SIS, ECRIS, SIV (Sistema de información de visados), URODAC (Sistema de comparación de huellas dactilares) o el SIA (Sistema de información aduanera)[11].

Ante tan ingente cuerpo normativo, ciertamente consideramos que la DM de 2008 procuró al menos establecer una serie de principios rectores en orden al tratamiento y protección de datos en causas criminales, siempre en la confianza de que esos mínimos facilitarían la cooperación judicial y policial transfronteriza.

Y es que el principio de disponibilidad, para la cooperación judicial y policial, necesita de una regulación por varias razones. Por un lado para poner orden en la enorme relación de normas que directa o indirectamente afectan a la materia, desde las de naturaleza aduanera hasta las que regulan el decomiso, pasando por el acceso a base de datos de ADN o de datos dactiloscópicos; evitando así regulaciones contradictorias,

---

[11] Una relación de estos instrumentos, en FIODOROVA, *"La transmisión..."*, op. cit., pp. 134 y 135. Igualmente, BAYO DELGADO – GUTIERREZ ZARZA – MICHAEL ALEXANDER, *"Intercambio de información, protección de datos y cooperación judicial penal"*, en VVAA (coord. por GUTIERREZ ZARZA), *Nuevas tecnologías...*, op. cit., pp. 195 y ss.

regímenes de autoridades competentes dispares, criterios objetivos y subjetivos diferentes a la hora de implementar medidas para recabar, almacenar y transmitir datos personales, y procedimientos de solicitud y transmisión distintos y con formularios también diferentes, lo que complica y ralentiza la labor policial y judicial.

Y, por otro lado, es precisa la regulación del principio de disponibilidad ante la necesidad de homogeneizar las garantías de las personas afectadas por estos procedimientos, como una base sólida y eficaz para la cooperación transfronteriza, como veremos más adelante.

Así, la DM de 2008 prevé la necesidad de articular normas comunes sobre el tratamiento posterior de los datos cedidos, una vez concluido su uso en la causa penal o investigación penal, así como sobre el tiempo de conservación de los datos, y su transmisión posterior a particulares.

E, igualmente, prevé la necesidad de normas comunes sobre confidencialidad y seguridad en el tratamiento de los datos cedidos, así como de normas comunes que garanticen un adecuado nivel de protección. Entre otras garantías, se menciona la información al interesado sobre la obtención de los datos, recopilación, tratamiento y cesión a otro Estado a efectos de investigación o enjuiciamiento penal, y sus consiguientes excepciones en aras de la consecución de los propios fines del intercambio, es decir, la investigación o el enjuiciamiento del delito.

Pero a pesar de todo ello, la DM de 2008 tuvo escaso éxito. Y ello, a nuestro modo de ver, por tres razones.

La primera, la naturaleza y alcance del propio instrumento normativo, la DM, que no tenía efecto directo en los ordenamientos de los Estados, lo que daba lugar a grandes diferencias en la materia a la hora de la transposición a los ordenamientos internos, y por tanto a la falta de la armonización normativa buscada.

La segunda, y como en tantas ocasiones, la limitación de la DM al ámbito transfronterizo, regulando el intercambio de datos entre Estados miembros y autoridades y sistemas de información europeos, pero sin que fuera vinculante para los asuntos internos de los Estados. Por tanto, se excluyen del ámbito de aplicación de la DM la recopilación y el tratamiento de los datos nacionales o "domésticos". Ello daría lugar a la divergencia entre los estándares de garantías establecidos en la DM respecto a la transferencia transfronteriza de datos personales, y el nivel garantista del

Derecho interno para su tratamiento dentro del propio Estado. Aunque la propia DM indica que el intercambio de datos a efectos penales se facilita cuando los Estados garantizan que el nivel de protección interno es el mismo que el de la DM para temas transfronterizos, sin embargo la misma no puede impedir que los Estados establezcan garantías mayores, aunque ello en principio no debe impedir ni obstaculizar la cooperación transfronteriza. No debe obstaculizarla, pero lo hace, ya que la DM no era un instrumento de aproximación normativa sino de establecimiento de mínimos para asuntos transfronterizos.

Y, la tercera, la circunstancia de que la DM de 2008 no estableciera el principio de especialidad. Aunque el art. 3 de la DM, como veíamos anteriormente, se refiere a un tratamiento lícito, adecuado, pertinente y no excesivo de los datos personales (principios de legalidad, finalidad y proporcionalidad), y a pesar de que se afirma que los datos sólo podrán utilizarse para el fin para el que se recabaron, tanto el art. 3.2 como el art. 11 de la DM permiten el tratamiento de dichos datos para otros fines o usos compatibles, de manera que el Estado receptor podría usar dichos datos, sin el consentimiento del sujeto afectado ni del Estado cedente, para otras finalidades diferentes de las que fundamentaron la transmisión, por ejemplo para la investigación o enjuiciamiento de otro delito, la ejecución de una pena, o en caso de graves e inmediatas amenazas a la seguridad pública. E incluso, el art. 13 prevé en el mismo sentido la transferencia a un tercer Estado, aunque en este caso se requiere el consentimiento del Estado que cedió inicialmente los datos.

A nuestro entender, esta posibilidad de que el Estado cesionario utilice los datos obtenidos para otros fines y para la investigación y enjuiciamiento de otros delitos, directamente relacionados o no con aquellos para cuya investigación y enjuiciamiento se cedieron, aunque parece responder al principio de proporcionalidad y necesariedad, sin embargo desconoce el principio de especialidad, lo que conlleva un grave déficit de garantías para el sujeto sospechoso o acusado, y, además, puede dar lugar a graves reticencias por parte del Estado cedente.

Por tanto, la DM de 2008 no sólo no establecía el principio de especialidad, sino que, como vemos, permitía la utilización de los datos transmitidos para para otros fines previstos en el Derecho interno, a diferencia incluso de instrumentos posteriores, como la antes citada DM

2009/315/JAI,[12] sobre intercambio de antecedentes penales (sistema ECRIS), cuyo art. 9, que establece las condiciones de uso de los datos de carácter personal, dispone que los datos de carácter personal comunicados para su uso en un procedimiento penal (supuestos del art. 7.1 de la DM) solo podrán ser utilizados por el Estado miembro requirente en el marco del procedimiento penal para el cual se solicitaron.

Incluso los datos de carácter personal comunicados para su uso fuera de un procedimiento penal, solo podrán ser utilizados por el Estado miembro requirente, con arreglo a su Derecho nacional, para los fines para los que los haya solicitado y dentro de los límites especificados por el Estado miembro requerido (art. 9.2 de la DM 2009/315).

Además, se prevé en el art. 9.3 de esta DM, que los Estados miembros adoptarán las medidas oportunas para garantizar que, si se transmiten a un tercer país datos de carácter personal que hayan recibido de otro Estado miembro, dichos datos estén sujetos a las mismas restricciones de utilización aplicables en un Estado miembro requirente del art. 9.2. Los Estados miembros especificarán que los datos personales que se transmitan a un tercer país a efectos de un procedimiento penal, solo podrán ser utilizados ulteriormente por dicho tercer país a efectos de un procedimiento penal[13].

Ante esta situación, el Programa de Estocolmo de 2010 a 2014, siguiendo la línea de la doble vía, la general de protección, y la excepcional y especial en materia de represión del delito, prevé la necesidad, por una parte, de un nuevo Reglamento general de protección de datos personales, que sustituyese a la Directiva de 1995 y, por otra, de una nueva Directiva sobre transmisión de datos personales en la cooperación penal, que vendría igualmente a sustituir a la citada DM de 2008.

Obviamente, al tratarse de una Directiva y no ya de una DM, el efecto armonizador sería más potente. E igualmente, se trataba de

---

[12] DM 2009/315/JAI del Consejo, de 26 de febrero de 2009, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros (DO L93 de 7 de abril de 2009).

[13] V. BLANCO QUINTANA, "*La comunicación de antecedentes penales entre los Estados. El Sistema europeo de información de antecedentes penales*", en BMJ, 2013, p. 23

fomentar que el instrumento no se limitase a reglamentar únicamente los intercambios transfronterizos de datos, sino que a través de la aproximación normativa también fuera aplicable al tratamiento interno de datos a efectos penales, estableciéndose el mismo nivel o estándar garantista para cualquier asunto penal, interno o transnacional.

No pasaban desapercibidas algunas cuestiones esenciales en esta proyectada aproximación normativa, como la transmisión de datos a autoridades de terceros países de la UE, y por tanto el distinto nivel garantista en los mismos. O, la posibilidad de excepcionar el principio de especialidad, es decir, establecer si el dato personal cedido a otro Estado a efectos penales, podía usarse para otros fines que, aunque legítimos, fueran ajenos al proceso penal en curso.

3 LA DOCTRINA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA SOBRE LOS PRINCIPIOS DE DISPONIBILIDAD Y PROPORCIONALIDAD EN LA OBTENCIÓN Y CESIÓN DE LOS DATOS PERSONALES

Las líneas esenciales de esa nueva proyectada Directiva sobre cesión y tratamiento de datos personales en materia de cooperación judicial penal en la UE, vienen expuestas fundamentalmente en tres Sentencias del TJUE.

La primera es la STJUE de 8 de abril de 2014, que resuelve varias cuestiones prejudiciales acumuladas (asuntos C-293/12 y C-594/12), planteadas respectivamente por la Corte Suprema de Irlanda y el TC de Austria[14]. Y la segunda, la STJUE de 21 de diciembre de 2016 (asuntos acumulados C-203/15 -Tele2 Sverige AB/Post-och telestyrelsen- y C-698/15 -Secretary of State for the Home Departament/Tom Watson y otros-). Más recientemente, la STJUE de 2 de octubre de 2018 (asunto

[14] Tribunal de Justicia de la Unión Europea, Gran Sala, Sentencia de 8 de abril de 2014, C-293/2012, Repertorio mensual de jurisprudencia, nº 6, 2014, p. 5.

Una completa exposición de las cuestiones prejudiciales irlandesa y austriaca en GONZÁLEZ PASCUAL, *"El TJUE como garante de los derechos de la UE a la luz de la Sentencia Digital Right Ireland",* en Revista de Derecho Comunitario Europeo, nº 49, 2014, pp. 943 y ss.

c 207/16), que resuelve una petición de decisión prejudicial planteada por la Audiencia Provincial de Tarragona.

A) En la STJUE de 8 de abril de 2014, estas cuestiones se centraban en la adecuación de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones[15], a los arts. 7, 8 y 11 de la Carta de Derechos fundamentales de la UE (en adelante, CDFUE), que establecen el derecho a la vida privada y la intimidad, a la protección de los datos personales y a la libertad de expresión.

Se trataba pues de examinar si el almacenamiento generalizado de datos de telecomunicaciones y retención de datos externos de las comunicaciones de los clientes por los proveedores de servicios, en orden a su posible tratamiento y posterior utilización en investigaciones penales[16], implicaban una intromisión ilegítima en los derechos a la intimidad y a la protección de datos personales.

El TJUE parte de que la Directiva de 2006 incide y afecta, mediante su intromisión y limitación, en tales derechos. Ahora bien, también apunta que la represión del delito, y por tanto, su investigación y enjuiciamiento, es un objetivo legítimo y de interés general, que justifica la limitación de los derechos en juego y la interferencia en su disfrute, sin que ello en principio implique una vulneración de los derechos concernidos.

El TJUE estima pues que la Directiva de 2006 afectaba a los derechos a la protección de datos y a la intimidad, aunque sin

---

[15] DO L 105, de 13 de abril de 2006. La Directiva de 2006 anulada por el TJUE, modificó en su momento la Directiva 2002/58/CE de 12 de julio de 2002 sobre tratamiento de datos personales y protección a la intimidad en el sector de comunicaciones electrónicas.

[16] Se establecía un sistema de tratamiento y almacenamiento de datos provenientes de las comunicaciones electrónicas de clientes de redes de acceso público. Este tratamiento y almacenamiento se encomendaba a las empresas encargadas de la prestación de los servicios de comunicaciones electrónicas, a efectos de que si fuera necesario se utilizaran los datos en investigaciones penales de delitos graves. El almacenamiento se establecía por un plazo de entre 6 a 24 meses.

lesionar sus contenidos esenciales, ya que las medidas de retención no implicaban el acceso al contenido de las comunicaciones (aunque si a la manera de rastrear el origen y destino de una comunicación, fecha y hora de la misma, su duración, el equipo del usuario y su localización, nombre y dirección del abonado, números de teléfono de origen y destino y en su caso dirección IP), y existían medidas en la norma para preservar ante posibles abusos en el uso de los datos por parte de las empresas.

Pero estas limitaciones o injerencias en los derechos a la intimidad y a la protección de los datos personales deben responder a unos principios rectores que son los que legitiman su uso para investigar y enjuiciar el delito. Por una parte, debe tratarse de medidas adecuadas y de previa configuración legal. Y, por otra, estas limitaciones responderán en todo caso al principio de proporcionalidad, por lo que la limitación o injerencia en el derecho debe adecuarse a la finalidad que la justifica, es decir, debe ser idónea; y, además, dicha limitación debe ser necesaria en orden a los fines de la investigación y el enjuiciamiento.

El TJUE entendió que había tres filtros que debía superar la Directiva de 2006. El primero, si afectaba, vulnerándolos, a los derechos fundamentales en cuestión; el segundo, si la Directiva pretendía la consecución de un interés general legítimo, la lucha contra la delincuencia grave; y, el tercero, si la Directiva era adecuada y necesaria para conseguir ese fin legítimo. La Directiva superó los dos primeros filtros, pero no el tercero, el juicio de proporcionalidad.

En tal sentido, la Sentencia de 2014 apuntaba como la Directiva de 2006 establecía medidas adecuadas de injerencia en los derechos fundamentales apuntados, en cuanto a su previsión legal general y en cuanto a que los fines perseguidos no implicaban en sí mismos una vulneración de tales derechos. Pero, sin embargo, estas medidas no se ajustaban a los cánones de proporcionalidad por varias razones.

El sistema de captación, recopilación y almacenamiento de datos se llevaba a cabo aún sin indicio penal alguno de comisión de un delito, y sin un catálogo preestablecido de delitos para los que podía acudirse a estas medidas, no siendo suficiente, a juicio del Tribunal, la referencia de la Directiva a delitos graves, sin ninguna otra precisión, catálogo o criterio al respecto.

En definitiva, el TJUE estableció cinco criterios esenciales sobre el principio de proporcionalidad, referido a la disponibilidad a efectos penales de los datos personales.

a) En primer lugar, el principio de disponibilidad en orden a la captación y almacenamiento de datos orientadas a la investigación y el enjuiciamiento penal, debe convivir con el respeto a los derechos fundamentales (intimidad y protección de datos personales), a través del establecimiento del principio de proporcionalidad, de manera que tales medidas respondan a los parámetros de necesidad e idoneidad.

b) En segundo lugar, es necesario preestablecer legalmente los datos objetivos y subjetivos en función de los cuales pueda justificarse la necesidad de estas medidas, es decir, la existencia de indicios contra la persona sospechosa o investigada, la discriminación en función de la persona afectada, la localización geográfica que precise el uso de la medida, el tiempo necesario para conservar los datos, etc., más allá de la genérica cláusula de la lucha contra delitos graves, que no aporta en sí misma ningún nexo de unión entre los datos que se obtengan y la finalidad perseguida.

c) En tercer lugar, es precisa también la existencia de un órgano autónomo que autorice o limite el acceso a los datos, exigencia que tampoco cumplía la Directiva.

d) En cuarto lugar, debe establecerse un marco de seguridad y protección suficiente, atendiendo a la cantidad de datos, su posible carácter sensible o los riesgos de acceso ilícito o de abusos al respecto. En tal sentido, con arreglo a la Directiva, las medidas de seguridad adecuadas de los proveedores de servicios para evitar abusos dependían de la valoración de los costes económicos para su implantación, lo cual no garantizaba la misma.

e) Y, en quinto lugar, la disponibilidad debe adecuarse al principio de especialidad, de manera que los datos recabados y cedidos lo sean en función de una causa penal concreta, en cuyo curso y sustanciación se pide la cooperación.

El principio de especialidad, que exige la relación de la investigación con un delito concreto, no impide, sin embargo, el trasvase o cesión de los datos personales recabados en una causa a otro proceso penal, con arreglo

al art. 579 bis de la LECRIM. Ello queda condicionado a la constatación de la legitimidad de la injerencia en los derechos fundamentales del investigado llevada a cabo en la primera causa. Pero dicha legitimidad para el trasvase de la información, también debería hacerse depender de otra circunstancia relevante, que no es otra que la concurrencia en la segunda causa de los presupuestos del art. 588 bis a., es decir, la procedencia (necesidad, excepcionalidad, idoneidad, etc.) en el segundo procedimiento de la medida de investigación que conduce a tales datos o informaciones[17]. Si en el segundo proceso no hubiera sido posible acordar, por ejemplo, la medida de registro remoto del equipo informático, por no tratarse de ninguno de los delitos del art. 588 septies a. de la LECRIM, ¿podría incorporarse la información obtenida con esta medida en la primera causa, sin ponderar si tal medida hubiera sido posible decidirla en el segundo proceso? A nuestro entender habría que contestar negativamente a la pregunta, de manera que sería preciso valorar la legitimidad de la adopción de la medida en el proceso de origen y en el segundo proceso. E idéntica solución en orden a la doble ponderación de la legitimidad de la medida, entendemos debe aplicarse en el ámbito de la cooperación transfronteriza.

B) Por su parte, la STJUE de 21 de diciembre de 2016, viene a resolver varias cuestiones prejudiciales acumuladas. Al día siguiente del pronunciamiento de la sentencia Digital Rights Ireland de 2014, la empresa de telecomunicación Tele2 Sverige notificó a la autoridad sueca de control de los servicios de correos y telecomunicaciones su decisión de no seguir conservando los datos y su intención de suprimir los datos ya registrados (asunto C-203/15). El Derecho sueco obliga en efecto a los proveedores de servicios de comunicaciones electrónicas a conservar de modo sistemático y continuado, sin ninguna excepción, todos los datos de tráfico y de localización de todos sus abonados y usuarios registrados en relación con todos los medios de comunicación electrónica. Por su parte, en el asunto C-698/15, los Sres. Tom Watson, Peter Brice y Geoffrey Lewis

[17] Problema que apunta COLOMER HERNÁNDEZ, *"La inclinación de la problemática provocada por la transmisión y cesión de datos personales obtenidos en un proceso penal desde el marco normativo comunitaria a la regulación y praxis española"*, en VVAA, (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales*..., op. cit., p. 838.

interpusieron recursos contra la normativa británica de conservación de datos que permite al Ministro del Interior obligar a los operadores de telecomunicaciones públicas a conservar todos los datos relativos a las comunicaciones durante un período máximo de doce meses, estando excluida la conservación del contenido de esas comunicaciones.

El Kammarrätten i Stockholm (Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo) y la Court of Appeal, England and Wales, Civil Division (Tribunal de Apelación del Reino Unido), solicitan al TJUE que indique si las normativas nacionales que imponen a los proveedores una obligación general de conservación de datos y que prevén el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar este acceso a los casos de lucha contra la delincuencia grave y sin supeditar el acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, son compatibles con el Derecho de la Unión (en el presente caso, la Directiva sobre la privacidad y las comunicaciones electrónicas, interpretada a la luz de la CDFUE).

La STJUE de 21 de diciembre de 2016, viene a establecer que los Estados miembros no pueden imponer una obligación general de conservación de datos de comunicaciones y geolocalización (datos de tráfico y localización), a los proveedores de servicios de comunicaciones electrónicas.

Y ello, básicamente, porque la conservación y almacenamiento de dichos datos personales, a efectos de prevención y persecución del delito, además de por razones relativas a la seguridad pública y nacional, incide en derechos fundamentales. Por ello, hay que conceptuarlo como un instrumento excepcional, que sólo puede utilizarse en casos tasados y con arreglo al principio de proporcionalidad, sin que quepan justificaciones abstractas como la referencia a delincuencia grave, que o bien se especifica en la Ley o debe ser objeto de interpretación individualizada en el caso concreto.

a) En definitiva, en virtud del principio de especialidad, el Derecho de la UE se opone a una conservación generalizada e indiferenciada de los datos de tráfico y de localización, pero los Estados miembros podrán establecer, con carácter preventivo, una conservación selectiva de esos

datos con la única finalidad de luchar contra la delincuencia grave, siempre que tal conservación se limite a lo estrictamente necesario por lo que se refiere a las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido. El acceso de las autoridades nacionales a los datos conservados debe estar sujeto a requisitos, entre los que se encuentran en particular un control previo por una autoridad independiente, así como la conservación de los datos en el territorio de la Unión.

b) Por lo que se refiere al acceso de las autoridades nacionales competentes a los datos conservados, el TJUE confirma que la normativa nacional no puede limitarse a exigir que el acceso responda a alguno de los objetivos contemplados en la Directiva, ni siquiera el de la lucha contra la delincuencia grave, sino que debe establecer también los requisitos materiales y procedimentales que regulen el acceso de las autoridades nacionales competentes a los datos conservados.

Esta normativa debe basarse en criterios objetivos para definir las circunstancias y los requisitos conforme a los cuales debe concederse a las autoridades nacionales competentes el acceso a los datos. En principio sólo podrá concederse un acceso, en relación con el objetivo de la lucha contra la delincuencia, a los datos de personas de las que se sospeche que planean, van a cometer o han cometido un delito grave o que puedan estar implicadas de un modo u otro en un delito grave.

No obstante, en situaciones particulares, como aquellas en las que intereses vitales de la seguridad nacional, la defensa o la seguridad pública estén amenazados por actividades terroristas, podría igualmente concederse el acceso a los datos de otras personas cuando existan elementos objetivos que permitan considerar que esos datos podrían, en un caso concreto, contribuir de modo efectivo a la lucha contra tales actividades.

c) En nuestro ordenamiento, será igualmente el Juez el que autorice la incorporación o cesión a la causa de los datos electrónicos de tráfico o asociados, conservados por los prestadores de servicios en cumplimiento de las normas de conservación, o bien por iniciativa de la Policía o del Ministerio Fiscal (art. 588 octies), o por propia iniciativa comercial (art. 588 ter de la LECRIM). Los proveedores de servicios de comunicaciones no están pues obligados a una conservación general de datos de sus usuarios.

Así, el art. 588 octies de la LECRIM, constitutivo del capítulo X (medidas de aseguramiento) del Título VIII (medidas de investigación limitativas de los derechos del art. 18 de la CE, establece la llamada "orden de conservación de datos", emitida por la Policía Judicial o por el Ministerio Fiscal a fin de requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición, hasta que se obtenga la autorización judicial correspondiente para su cesión. Los datos se conservarán durante un período máximo de 90 días, prorrogable una sola vez hasta que se obtenga la autorización judicial de la cesión o se cumplan 180 días. El requerido vendrá obligado a prestar la colaboración y asistencia, y a guardar secreto sobre esta diligencia, con arreglo al art. 588 ter e. de la LECRIM.

Por su parte, el art. 588 ter j. (datos obrantes en archivos automatizados de los prestadores de servicios), dispone que los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial. Igualmente, cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

C) En tercer lugar, nos referimos a la STJUE de 2 de octubre de 2018 (asunto C 207/16), que resuelve una petición de decisión prejudicial planteada por la Audiencia Provincial de Tarragona, en un proceso penal incoado por el Ministerio Fiscal. En la misma, como veremos a continuación, se analiza el criterio relativo a la gravedad del delito, en orden a la legitimidad o justificación de la injerencia en los derechos fundamentales reconocidos en los arts. 7 y 8 de la CDFUE, y si hay que atender únicamente a la pena que pueda imponerse al delito que

se investiga o es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos.

Los hechos de los que trae causa el proceso en España, parten de una denuncia presentada ante la Policía por un robo con violencia, durante el cual el denunciante resultó herido y le sustrajeron la cartera y el teléfono móvil. La Policía Judicial presentó un oficio ante el juez instructor solicitando que se ordenase a diversos proveedores de servicios de comunicaciones electrónicas la transmisión de los números de teléfono activados, desde el 16 de febrero hasta el 27 de febrero de 2015, con el código relativo a la identidad internacional del equipo móvil (en adelante, código IMEI) del teléfono móvil sustraído, así como los datos personales o de filiación de los titulares o usuarios de los números de teléfono correspondientes a las tarjetas SIM activadas con dicho código, como su nombre, apellidos y, en su caso, dirección.

El juez instructor denegó la diligencia solicitada por dos motivos. Por un lado, consideró que esta no era idónea para identificar a los autores del delito. Por otra parte, denegó la solicitud porque la Ley 25/2007, de 28 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, limitaba la cesión de los datos conservados por las operadoras de telefonía a los delitos graves, que, con arreglo a los arts. 13.1 y 33.1 del Código Penal (en adelante, CP), son, entre otros, los sancionados con una pena de prisión superior a cinco años, siendo que los hechos investigados no parecían ser constitutivos de delito grave.

El Ministerio Fiscal interpuso recurso de apelación contra dicho auto ante la Audiencia Provincial, alegando que, dada la naturaleza de los hechos y habida cuenta de una sentencia del Tribunal Supremo, de 26 de julio de 2010, relativa a un caso similar, debería haberse acordado la cesión de los datos de que se trata. Al respecto hay que tener en cuenta que tras los hechos de los que trae causa esta cuestión prejudicial, y con posterioridad a dicho auto de la AP, la LO 13/2015, de 5 de octubre, de modificación de la LECRIM, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas, supuso, atendiendo a la jurisprudencia del TC y del TS, la introducción respecto de determinadas medidas de investigación, de dos nuevos

criterios alternativos para determinar el nivel de gravedad de un delito y, por tanto, establecer dicha gravedad como presupuesto para autorizar la medida. Se trata, por un lado, de un estándar material identificado por conductas típicas de particular y grave relevancia criminógena que incorporan particulares tasas de lesividad para bienes jurídicos individuales y colectivos, tales como los delitos cometidos en el seno de organizaciones criminales o en materia de terrorismo. Por otro, la LECRIM ha introducido un criterio normativo - formal basado en la pena prevista para el delito de que se trate, de manera que hay medidas de investigación tecnológica que sólo pueden decretarse respecto a delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión (así, con arreglo a los arts. 579.1.1º y 588 ter a. de la LECRIM respecto a la interceptación de comunicaciones telefónicas y telemáticas).

Todo ello, como alega la AP, sin perjuicio de que el interés del Estado en castigar las conductas infractoras no puede justificar injerencias desproporcionadas en los derechos fundamentales consagrados en la CDFUE. Además, al plantear la cuestión prejudicial, la AP de Tarragona afirma que la STJUE de 8 de abril de 2014 -caso Digital Rights Ireland y otros- declaró la invalidez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, reconociendo el TJUE que la conservación y cesión de datos de tráfico constituyen injerencias especialmente graves en los derechos garantizados por los arts. 7 y 8 de la CDFUE, e identificando los criterios de apreciación del respeto del principio de proporcionalidad, entre ellos la gravedad de los delitos que justifican la conservación de estos datos y el acceso a ellos para la investigación de un delito.

Las cuestiones prejudiciales planteadas, y que son el objeto de la sentencia, son dos, y giran en torno al principio de proporcionalidad en su vertiente de gravedad del delito investigado u objeto de acusación y enjuiciamiento, como elemento determinante de la legitimidad del acceso a los datos personales derivados de comunicaciones electrónicas (datos personales de tráfico y geolocalización). De esta manera se pregunta al TJUE:

a) ¿Cómo se identifica el criterio relativo a la gravedad del delito, en orden a la legitimidad o justificación de la injerencia en los derechos

fundamentales reconocidos en los arts. 7 y 8 de la CDFUE? ¿Hay que atender únicamente a la pena que pueda imponerse al delito que se investiga o es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos?

b) En su caso, si se ajustara a los principios constitucionales de la UE, utilizados por la STJUE de 8 de abril de 2014 (Digital Rights Ireland y otros) como estándares de control estricto de la Directiva de 2002 antes citada, y la determinación de la gravedad del delito atendiera solo a la pena imponible, ¿cuál debería ser ese umbral mínimo? ¿Sería compatible con una previsión general de límite en tres años de prisión?

Con carácter inicial, el TJUE recuerda que el acceso de las autoridades públicas a estos datos personales, constituye una injerencia en el derecho fundamental al respeto de la vida privada, consagrado en el art. 7 de la CDFUE, incluso a falta de circunstancias que permitan calificar esta injerencia de «grave», y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible, o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia. Tal acceso también constituye una injerencia en el derecho fundamental a la protección de los datos personales garantizado por el art. 8 de la CDFUE, puesto que constituye un tratamiento de dichos datos.

Ahora bien, por lo que respecta a los objetivos que pueden justificar una norma nacional, como la controvertida en el litigio principal, que regula el acceso de las autoridades públicas a los datos conservados por los proveedores de servicios de comunicaciones electrónicas y, por tanto, establece una excepción al principio de confidencialidad de las comunicaciones electrónicas (Ley 25/2007, de 18 de octubre), es resaltable que la enumeración de los objetivos que figuran en el art. 15.1, primera frase, de la Directiva 2002/58, tiene carácter exhaustivo, de modo que dicho acceso ha de responder efectiva y estrictamente a uno de ellos (en este sentido, la STJUE 21 de diciembre de 2016 (Tele2 Sverige y Watson y otros, apartados 90 y 115). Siendo el objetivo la prevención, investigación, descubrimiento y persecución de delitos, procede observar que el tenor del art. 15. 1, primera frase, de la Directiva 2002/58 no limita este objetivo a la lucha contra los delitos graves, sino que se refiere a los «delitos» en general.

A este respecto, es cierto que el TJUE ha declarado que, en materia de prevención, investigación, descubrimiento y persecución de delitos, solo la lucha contra la delincuencia grave puede justificar un acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas que, considerados en su conjunto, permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados (STJUE de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, apartados 99 y 115). El TJUE ha motivado esa interpretación basándose en que el objetivo perseguido por una norma que regula este acceso, debe guardar relación con la gravedad de la injerencia en los derechos fundamentales en cuestión.

Es decir, conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos solo puede justificar una injerencia grave, el objetivo de luchar contra la delincuencia que a su vez esté también calificada de «grave». Pero cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general.

Por tanto, el TJUE se plantea si en el presente asunto, en función de las circunstancias del caso de autos, la injerencia en los derechos fundamentales reconocidos en los arts. 7 y 8 de la CDFUE, que entraña el acceso de la Policía Judicial a los datos de que se trata en el litigio principal, debe considerarse «grave». A este respecto, el oficio por el que la Policía Judicial solicita, a efectos de la investigación de un delito, autorización judicial para acceder a los datos personales conservados por los proveedores de servicios de comunicaciones electrónicas, tiene por único objeto identificar a los titulares de las tarjetas SIM activadas, durante un período de doce días, con el número IMEI del teléfono móvil sustraído. De este modo, esta solicitud no tiene más objeto que el acceso a los números de teléfono correspondientes a las tarjetas SIM, así como a los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre, apellidos y, en su caso, la dirección. En cambio, esos datos no se refieren a las comunicaciones efectuadas con el teléfono móvil sustraído ni a la localización de este.

Así, los datos a que se refiere la solicitud de acceso controvertida en el litigio principal, sólo permiten vincular, durante un período

determinado de doce días, la tarjeta o tarjetas SIM activadas con el teléfono móvil sustraído y los datos personales o de filiación de los titulares de estas tarjetas SIM. Sin un cotejo con los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y de localización, estos datos no permiten conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas con las tarjetas SIM en cuestión, ni los lugares en que estas comunicaciones tuvieron lugar, ni la frecuencia de estas con determinadas personas durante un período concreto. Por tanto, dichos datos no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados.

En tales circunstancias, el acceso limitado únicamente a los datos cubiertos por la solicitud controvertida en el litigio principal, no puede calificarse de injerencia «grave» en los derechos fundamentales de los individuos cuyos datos se ven afectados. En consecuencia, la injerencia que supone el acceso a dichos datos puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general, objetivo al que se refiere el art. 15. 1, primera frase, de la Directiva 2002/58, sin que sea necesario que dichos delitos estén calificados como «graves».

Habida cuenta de las consideraciones anteriores, con arreglo al art. 15, apartado 1, de la Directiva 2002/58, a la luz de los arts. 7 y 8 de la CDFUE, el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

En virtud de todo lo expuesto, el TJUE (Gran Sala) declara que el art. 15.1 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, a la luz de los arts. 7 y 8 de la CDFUE, debe interpretarse en el sentido de que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares

de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

Como decíamos más arriba, hay que tener presente que con posterioridad a los hechos del litigio principal, la LECRIM ha sido modificada por la LO 13/2015, de 5 de octubre, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Dicha Ley, que entró en vigor el 6 de diciembre de 2015, reforma la intervención de comunicaciones telefónicas y telemáticas, e introduce en la LECRIM la cuestión del acceso a los datos relativos a las comunicaciones telefónicas y telemáticas conservados por los proveedores de servicios de comunicaciones electrónicas, con arreglo a lo previsto en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Así, el art. 588 ter a., sobre interceptación de comunicaciones telefónicas y telemáticas, en su versión resultante de la LO 13/2015, dispone, por remisión al art. 579.1.1º, que esta medida puede decretarse siempre que la investigación tenga por objeto alguno de los siguientes delitos: 1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; 2.º Delitos cometidos en el seno de un grupo u organización criminal; y, 3.º Delitos de terrorismo.

Por tanto, y salvo en casos de delitos cometidos en el seno de grupo u organización criminal o en los delitos de terrorismo, sólo cabría la interceptación de comunicaciones telefónicas y telemáticas respecto a delitos con límite máximo de al menos 3 años de prisión.

Advertimos pues que estamos ante una injerencia grave en los derechos fundamentales del investigado, que requiere venir referida a la investigación de un delito "grave", en el sentido que apunta la STJUE de 2 de octubre de 2018, tal y como lo defina la legislación estatal, e independientemente, al parecer, del concepto formal de delito grave de los arts. 13.1 y 33.1 del CP. Dicha gravedad se configura, como presupuesto de la medida de investigación, atendiendo pues a dos criterios alternativos

para determinar el nivel de gravedad de un delito y, por tanto, establecer dicha gravedad como presupuesto para autorizar la injerencia grave en los derechos fundamentales. Se trata, por un lado, de un estándar material identificado por conductas típicas de particular y grave relevancia criminógena, tales como los delitos cometidos en el seno de organizaciones criminales o en materia de terrorismo. Por otro, la LECRIM ha introducido un criterio normativo-formal basado en la pena prevista para el delito de que se trate, de manera que hay medidas de investigación tecnológica que sólo pueden decretarse respecto a delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión (así, con arreglo a los arts. 579.1.1º y 588 ter a de la LECRIM respecto a la interceptación de comunicaciones telefónicas y telemáticas). Este límite máximo de al menos tres años de prisión, actúa como presupuesto de la medida, y entendemos que prevalece respecto al establecido en el art. 1 de la Ley 25/2007, que se refiere a delito grave.

Por su parte, el art. 588 ter j) de la LECRIM establece que los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión. El precepto no exige ningún presupuesto relativo a la gravedad de la penalidad del delito investigado, lo que no implica que no deba ajustarse a la proporcionalidad general exigida en el art. 588 bis de la LECRIM en orden a la idoneidad, necesidad y excepcionalidad de la medida de investigación.

De esta manera, y con arreglo a la doctrina fijada por la STJUE de 2 de octubre de 2018, se trata de una injerencia que implica un acceso que no es grave, por lo que puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general.

Ahora bien, la entidad y alcance de las medidas previstas en el art. 588 ter j), incluye, no sólo las que son objeto del pleito principal del caso (acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares), que constituyen una injerencia en los derechos fundamentales de estos, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

También se refiere el citado precepto a otras medidas que sí podrían calificarse como injerencias graves, en orden a la afección de los derechos fundamentales de los arts. 7 y 8 de la CDFUE y 18 de la CE, como los datos de tráfico y datos de localización, respecto de los que, con arreglo al art. 1 de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, el acceso se condiciona a la autorización judicial previa y, además, a que se trate de la investigación de delitos graves, requisito éste último no incluido en el art. 588 ter j).

Por delincuencia grave, consideramos que deberá entenderse en este caso, delitos cometidos en el seno de organizaciones criminales o en materia de terrorismo, así como delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión, de manera que prevalece la configuración de delito grave de los arts. 579.1.1º y 588 ter de la LECRIM, respecto a la del art. 1 de la Ley 25/2007. Es decir, conforme al principio de proporcionalidad, tal y como lo configura la STJUE de 2 de octubre de 2018, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, las medidas del art. 588 ter j) incluye injerencias graves para luchar contra la delincuencia que a su vez esté también calificada de «grave», e injerencias que no son graves, y que por tanto se pueden decretar respecto a todo delito.

El TJUE ha declarado que, en materia de prevención, investigación, descubrimiento y persecución de delitos, solo la lucha contra la delincuencia grave puede justificar un acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas que, considerados en su conjunto, permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados (así, la STJUE

de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, apartados 99 y 115). El TJUE ha motivado esa interpretación basándose en que el objetivo perseguido por una norma que regula este acceso, debe guardar relación con la gravedad de la injerencia en los derechos fundamentales en cuestión que supone la operación.

Es decir, conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de «grave».

Pero, cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general. El art. 588 ter j) de la LECRIM no exige ningún presupuesto relativo a la gravedad de la penalidad del delito investigado, lo que no implica que no deba ajustarse a la proporcionalidad general exigida en el art. 588 bis de la LECRIM.

De esta manera, y con arreglo a la doctrina fijada por la STJUE de 2 de octubre de 2018, se trata de una injerencia que implica un acceso que no es grave, por lo que puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general.

Ahora bien, la entidad y alcance de las medidas previstas en el art. 588 ter j), incluye, no sólo las que son objeto del pleito principal del caso (acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares), que constituyen una injerencia en los derechos fundamentales de estos, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

También se refiere el citado precepto a otras medidas que sí podrían calificarse como injerencias graves, en orden a la afección de los derechos fundamentales de los arts. 7 y 8 de la CDFUE y 18 de la CE, como los datos de tráfico y datos de localización, respecto de los que, con arreglo al art. 1 de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, el acceso se condiciona a la autorización judicial previa y, además, a que se trate de la investigación de delitos graves, requisito

éste último no incluido en el art. 588 ter j), sin que pueda entenderse que el apartado 1 del precepto realice una remisión general a la legislación sobre retención de datos relativos a las comunicaciones electrónicas (Ley 25/2007).

Es decir, conforme al principio de proporcionalidad, tal y como lo configura la STJUE de 2 de octubre de 2018, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, las medidas del art. 588 ter j) incluye injerencias graves para luchar contra la delincuencia que a su vez esté también calificada de «grave», e injerencias que no son graves, y que por tanto se pueden decretar respecto a todo delito.

4. LA PROTECCIÓN DE LOS INTERESADOS EN EL TRATAMIENTO DE DATOS PERSONALES, PARA LA PREVENCIÓN, INVESTIGACIÓN, DETECCIÓN O ENJUICIAMIENTO PENAL. LA DIRECTIVA (UE) 2016/680 Y ALGUNAS REFLEXIONES SOBRE SU IMPACTO EN EL PROCESO PENAL ESPAÑOL

4.1. Ámbito de aplicación y principios rectores

La Directiva UE 2016/680, de 27 de abril de 2016[18], del Parlamento Europeo y del Consejo, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y sobre la libre circulación de dichos datos, que deroga la DM

[18] Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la DM 2008/977/JAI del Consejo (DO L 119 de 4 de mayo de 2016, p. 89).

2008/977[19] [20], responde a una serie de principios generales que parten de las líneas de actuación del Programa de Estocolmo, así como de los criterios del TJUE antes expuestos.

Entendemos que esta nueva regulación sobre el tratamiento y análisis de datos personales en causas penales, que ya trasciende del ámbito transfronterizo y parece optar por la aproximación normativa en orden a facilitar la cooperación judicial penal, trae causa de unos primeros trabajos de la Comisión Europea que datan de 2009[21] y que defienden una política más coherente e integradora del derecho fundamental a la protección de datos personales en todos los contextos. Estos trabajos

---

[19] Hay que hacer mención igualmente de la Directiva de 27 de abril de 2016 sobre utilización de datos del PNR (Registro de nombres de pasajeros), fundamentalmente en materia de terrorismo y formas graves de delincuencia, recogidas en un catálogo expreso, y encaminada a la prevención, detección, investigación y enjuiciamiento de tales delitos.

Se prevén en este sentido, cuatro formas de intercambio de este tipo de datos: entre las UIP (Unidad de Información de Pasajeros) de los Estados, directamente en casos de urgencia; entre las autoridades competente de los Estados y la UIP de un Estado requerido; a través del acceso de Europol a dichos registros con la colaboración de la UIP de los Estados; y, mediante la transferencia a terceros países.

[20] La DM de 2008 queda derogada con efecto a partir del 6 de mayo de 2018, fecha límite establecida para la transposición de la nueva Directiva 2016/680 (arts. 59 y 63).

[21] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Internet de los objetos. Un plan de acción para Europa,* de 18 de junio de 2009, COM (2009) 278 final. V. igualmente, *Programa de Estocolmo. Una Europa abierta y segura que sirva y proteja al ciudadano,* DO C 115 de 4 de mayo de 2010, p. 1; Comunicación de la Comisión *Un enfoque global de la protección de datos personales en la Unión Europea* COM (2010) 609 final. Hay que mencionar también las iniciativas sobre construcción del mercado digital único, entre cuyas acciones se menciona la necesidad de reforma normativa, con tres grandes finalidades: superar las divergencias en la implantación de la Directiva de 1995, adaptarse a los nuevos avances tecnológicos, y afrontar la dimensión globalizada del tratamiento de datos personales en el ámbito penal y policial, *European Data Protection Supervisor, Opinion on the data protection reform package,* de 7 de marzo de 2012 (cit, por VILLARINO MARZO, *"La Unión Europea ante los retos de la era digital…",* op. cit, p. 570).

fructifican en sendas propuestas legislativas en 2012[22], aunque habría que esperar a 2016 para ver culminados los trabajos y publicados, por una parte el Reglamento (UE) 2016/679, sobre protección de datos y, por otra, la Directiva (UE) 2016/680, sobre el tratamiento de datos personales en causas penales, a la que nos venimos refiriendo en estas páginas.

Durante estos años, no debemos olvidar que el TJUE y sus líneas maestras sobre los principios de legalidad y proporcionalidad, han influenciado decididamente la redacción de la nueva Directiva de 2016, aunque sin obviar esa orientación de política criminal centrada en el principio de disponibilidad de los datos personales a efectos penales, y el afán de compatibilizar una más eficaz persecución, investigación y enjuiciamiento del delito, aprovechando eficientemente los avances tecnológicos, con el respeto de los derechos fundamentales del titular de los datos personales, a la vez sospechoso, investigado o encausado.

En tal sentido, pasamos a continuación a exponer brevemente estos principios generales.

4.2. El principio de disponibilidad y libre circulación

La libre circulación de datos personales recogidos e intervenidos por las autoridades competentes de un Estado, debe responder a fines explícitos y legítimos de la cooperación judicial penal. Como afirma COLOMER HERNÁNDEZ[23], existe una especial vinculación entre la

---

[22] Propuesta de nuevo Reglamento sobre protección de datos -COM (2012) 11 final 2012/0011/COD-, y Propuesta de Directiva sobre tratamiento de datos personales para fines de investigación y enjuiciamiento -COM (2012) 10 final 2012/0010/COD- . V. GONZÁLEZ CANO, *"Algunas reflexiones sobre protección de datos personales, proceso penal y cooperación judicial penal en la Unión Europea",* op. cit.

[23] COLOMER HERNÁNDEZ, *"La inclinación de la problemática..."*, en VVAA, (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales...,* op. cit., p. 831. IDEM, *"La cesión de datos de las comunicaciones electrónicas para su uso en investigaciones criminales: una problemática en ciernes"*, en VVAA (dir. por JIMÉNEZ CONDE*), Adaptación del Derecho Procesal español a la normativa europea y su interpretación por los tribunales*, Tirant lo blanch, 2018, pp. 77 y ss.; RICHARD GONZÁLEZ, *"La conservación y utilización de datos de las comunicaciones en la investigación criminal. Problemas que resultan de la aplicación de la doctrina del TJUE"*, en VVAA, *Adaptación...,* op. cit. pp. 475 y ss.

finalidad para la que se recaba o recoge el dato personal y el uso que después se le da en el Estado requirente o cesionario, o incluso en un tercer Estado diferente del que solicitó la transmisión.

Así, se pone de manifiesto como la rapidez de la evolución tecnológica y la globalización conllevan nuevos retos respecto a la protección de los datos personales, en cuanto derecho fundamental con arreglo a los arts. 8, apartado I de la CDFUE, y 16, apartado I, del TUE. Pero, igualmente, esa masiva recogida e intercambio de datos, sin lugar a dudas supone un activo importante en la investigación y enjuiciamiento del delito.

La libre circulación de datos entre las autoridades competentes en la investigación y enjuiciamiento del delito, debe ser facilitada en el ámbito de la cooperación penal y como instrumento para la creación y fortalecimiento del espacio europeo de libertad, seguridad y justicia, aunque siempre en un marco sólido y coherente de protección y de garantías adecuadas y efectivas de los titulares de los datos personales.

Es pues evidente que la propia eficacia de la cooperación judicial penal depende de que previamente se cree y asegure en todos los Estados miembros, un nivel uniforme y equivalente de protección de los datos personales y de su tratamiento.

Si bien es cierto que el nuevo Reglamento general 2016/679[24], de protección de datos, establece las normas generales para la protección de las personas físicas en relación con el tratamiento de sus datos personales, y para garantizar la libre circulación de datos personales en la UE, también lo es que resulta imprescindible la elaboración de una serie de normas específicas sobre protección de datos y libre circulación de los mismos en el ámbito de la cooperación penal a la que se refiere el art. 16 del TUE, es decir, en orden a la investigación y enjuiciamiento de delitos por autoridades competentes (Jueces, Fiscales, Policía), y en general por todo organismo o entidad que tenga encomendado el tratamiento de estos datos a tales fines.

---

[24] Reglamento (UE) del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119, de 4 de mayo de 2016, p. 1.).

Téngase presente que la labor normativa de la UE en materia de protección de datos comenzó con la Directiva 1995/46/CE, intentando reforzar la libre circulación de datos personales en el marco del mercado único comunitario[25], dispensando para ello un marco de protección que se extendió a datos contenidos en soporte informático o en cualquier tipo de soporte o archivo adecuado o idóneo para su tratamiento. A partir de ahí, los avances tecnológicos por una parte y, por otra, la necesidad de la obtención y tratamiento de los datos personales en el ámbito de la cooperación judicial penal, han dado lugar, como afirma GALÁN MUÑOZ, a la doble vía de protección de los datos de carácter personal, es decir, la vía garantista general, en orden a preservar ante la libre circulación de datos personales, los derechos de información, acceso, rectificación, cancelación y oposición; y, la vía excepcional o especial, la relacionada con la represión, la investigación y el enjuiciamiento del delito, que requiere un tratamiento especial[26] en cuanto se trata de medios de investigación y obtención de fuentes probatorias preconstituidas y, en definitiva, de prueba de cargo en orden a la imposición de consecuencias jurídicas sancionadoras de naturaleza penal.

Aunque ciertamente los primeros pasos normativos se dieron en el ámbito general y garantista de la protección de datos personales en un mercado único con libre circulación de servicios, bienes y personas, realmente el desarrollo legislativo más importante se ha producido en el ámbito de la utilización de datos personales como material de investigación y preconstitución probatoria de cargo, tal y como hemos visto en páginas anteriores.

Se trata pues de garantizar un mismo nivel de protección en este ámbito de la cooperación judicial penal, normas armonizadas y aproximación normativa que no deben contribuir a debilitar los estándares de protección de los Estados. Muy al contrario, los Estados, partiendo de los mínimos que se establezcan, e independientemente de la nacionalidad o residencia del titular de los datos (Considerando 17 de la Directiva

---

[25] PARIENTE DE PRADA, *El Espacio de libertad, seguridad y justicia: Schenguen y protección de datos,* Aranzadi, Cizur Menor, 2013, pp. 127 y ss.

[26] Sobre la doble vía apuntada, v. igualmente, SOLAR CLAVO, *"La doble vía europea en protección de datos",* en La Ley, nº 2832, 2012.

2016/680), de que sea persona identificada o identificable, y de que se trate de tratamiento automatizado o no de los datos (neutralidad tecnológica para evitar el riesgo de elusión del estándar de protección, con arreglo al Considerando 18), podrán lógicamente disponer mayores garantías en sus ordenamientos. Igualmente, las normas procesales penales de los Estados miembros podrán contener sus propias prescripciones sobre obtención y tratamiento de datos personales en causas penales, así como sobre identificación, datos genéticos, relativos a la salud, económicos o financieros.

Por tanto, el ámbito de aplicación de la Directiva de 2016 se amplía en relación a la DM de 2008, aunque ello convive con algunas limitaciones, ya que la Directiva no se aplica al tratamiento de datos personales en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho de la UE, ni por parte de instituciones, órganos u organismos de la UE (art.2.3). Igualmente, la Directiva no es aplicable a actividades en materia de recogida y tratamiento de datos personales relacionadas con la seguridad nacional (Considerando 14), aunque hay que decir que la excepción relativa a los intereses de seguridad nacional, a pesar de quedar fuera de la cobertura de ese sistema coherente y uniforme de protección del sujeto, constituye o forma parte a su vez del régimen de excepciones o limitaciones del derecho de información o del derecho de acceso del interesado a los datos personales (arts. 13 y 15), sobre el que volveremos más adelante.

Sin embargo, consideramos positiva la previsión a la que se refiere el Considerando (25) de la Directiva 2016/680, que dispone la aplicabilidad de la Directiva a las transmisiones de datos desde los Estados de la UE a Interpol y a países donde la organización tiene destinados miembros. Así, la obtención, almacenamiento y distribución de datos personales para combatir la delincuencia internacional a través de intercambio de datos con Interpol, debe garantizar el respeto a los derechos y libertades fundamentales, básicamente en orden al tratamiento automatizado de los datos.

Igualmente, los principios de libre circulación y disponibilidad incluyen las transferencias de datos personales a terceros países u organizaciones internacionales. Así, el art. 35 establece los principios generales de estas transferencias de datos personales, que quedan condicionadas por cinco presupuestos.

a) Que la transferencia sea necesaria a los fines de la cesión y el tratamiento que con carácter general establece el art. 1.1, y sobre los que trataremos a continuación.

b) Que los datos personales se transfieran a un responsable del tratamiento de un tercer país u organización internacional que sea una autoridad pública competente a los fines mencionados en el art. 1.1.

c) Que, en caso de que los datos personales se transmitan o procedan de otro Estado miembro, dicho Estado miembro haya dado su autorización previa para la transferencia de conformidad con el Derecho nacional.

d) Que la Comisión haya adoptado una decisión de adecuación o de evaluación del nivel de protección en el Estado cesionario o, a falta de la misma, la transferencia se condicione a la aportación por dicho Estado de las garantías apropiadas (arts. 36 y 37). Y,

e) que se valore especialmente la proporcionalidad de la cesión en orden a todos los factores pertinentes, entre estos la gravedad de la infracción penal, la finalidad para la que se transfirieron inicialmente los datos personales, y el nivel de protección de los datos personales existente en el tercer país u organización internacional a los que se transfieran ulteriormente los datos personales.

¿Se ajusta nuestra jurisprudencia a las previsiones sobre el principio de disponibilidad de la Directiva de 2016? La STS de 23 de febrero de 2017 (STS 116/2017), ha avalado la condena por fraude fiscal, fundada en una prueba de cargo derivada directamente de la ilícita obtención de archivos informáticos por un particular (el Sr. Falciani), en los que se contenían datos de las cuentas bancarias del acusado.

La información sustraída por el Sr. Falciani (datos bancarios incluidos en listados del banco suizo HSBC), fue intervenida por la autoridad francesa en un registro judicial en su domicilio, previa petición de cooperación internacional por la autoridad de Suiza en la investigación de delitos contra el secreto bancario. Posteriormente estos datos (material incriminatorio inicialmente incautado para la causa penal en Suiza), fue remitida a la AEAT española mediante un DVD creado a partir de los referidos archivos informáticos aprehendidos en poder de Falciani, que contenían datos de los contribuyentes posteriormente acusados en España.

Se trata pues de dar validez como prueba de cargo a la información y datos personales obtenidos ilegitimamente por un particular en Suiza, posteriormente intervenida por un juez francés en la investigación de los delitos cometidos por dicho particular, previa petición de cooperación internacional por Suiza en la investigación de delitos contra el secreto bancario, y remitida a la autoridad española (la Agencia española de administración tributaria) que los pidió a la autoridad administrativa francesa en virtud del Convenio de 1995 para evitar la doble imposición y prevenir el fraude fiscal.

El Tribunal Supremo concluyó que la *lista Falciani* es prueba de cargo válida *por tener la convicción* de que, aunque los datos se obtuvieron de manera ilícita, la finalidad directa o indirecta no era de utilizarlos en un proceso, ni medió acuerdo o connivencia con las autoridades de ningún país.

Además de otras relevantes cuestiones dignas de ser analizadas en esta STS, tales como el alcance del principio de no indagación, la validación de la cadena de custodia, la aplicación de la regla de exclusión por la vulneración del derecho a la protección de datos en la obtención de la información, etc.[27], hay que convenir que la cesión de datos personales por parte de la autoridad francesa a la española, y su preconstitución como prueba de cargo, plantea algunas cuestiones relevantes a efectos de la persecución criminal.

a) En primer lugar, estamos ante un caso de cooperación judicial penal, para obtener de otro Estado datos personales para la investigación y el enjuiciamiento de un delito. Una cesión de datos (que el TS llega a calificar como mera denuncia ya que los datos provienen de un particular), que debe solicitarse atendiendo al principio de especialidad, en el curso de una causa abierta, y por los cauces oportunos de obtención de material

[27] La defensa del condenado había formulado recurso de casación alegando la doctrina según la cual las pruebas derivadas de una actuación ilegítima quedan contaminadas de dicha ilicitud y por tanto no son válidas como prueba de cargo para desvirtuar la presunción de inocencia del acusado. Sin embargo el TS ha entendido que puede constituir prueba de cargo válida y suficiente para fundar la condena, un elemento de convicción derivado de una actividad ilícita llevada a cabo por un particular, siempre que dicho elemento no se haya obtenido con la finalidad de utilizarlo en un proceso; y la persona que lo obtiene que no sea un agente encubierto o conectado con la policía o aparatos del Estado.

incriminatorio en un Estado distinto al del proceso (exhorto europeo o bien Orden Europa de investigación (en adelante, OEI).

El TS apunta que la utilización de estas pruebas para desvirtuar la presunción de inocencia requiere, por una parte, la convicción de que no hay intencionalidad procesal ni conexión policial alguna en la obtención de los datos, es decir que el particular no los sustrajo para sustentar una causa penal; y, por otra, que deberá ponderarse en cada caso, por un lado la gravedad de la lesión al derecho fundamental (en este caso intimidad y protección de datos) y la gravedad del delito descubierto (fraude fiscal).

Sin embargo, la desconfianza sobre los datos "traspasados", no se debe a quien los obtiene (un particular por motivos económicos o mediáticos, o la policía en el curso de una investigación), sino por la ilicitud de la obtención de los indicios y los datos, ya que la obtención y cesión no se fundamenta en los principios de disponibilidad, especialidad y proporcionalidad.

Dejamos pues planteadas nuestras dudas sobre la observancia en este caso de los contenidos mínimos del principio de especialidad, ya que la incautación de los archivos informáticos en Francia, trae causa de una petición de cooperación judicial de Suiza, país en el que se sigue la causa por los delitos contra el secreto bancario. La cesión de los datos a Suiza se realiza con un fin explícito y determinado, que no es otro que el enjuiciamiento del Sr. Falciani, y no el uso de tales datos en la causa posterior en España.

Aprovechar ese cauce de cooperación bilateral, por un delito concreto y con un imputado individualizado, para que la información acabe siendo prueba de cargo en un proceso posterior que se abre en un tercer Estado, España, supone una vulneración del principio de especialidad. La transferencia a España, y por tanto el uso de los datos para el mismo fin pero en otra causa penal por otros delitos y contra otros sujetos, está contemplada en el art. 4.2 de la Directiva 2016/680, al modo de una manifestación ampliada del principio de disponibilidad, pero siempre contando con la autorización previa de Suiza, país que inicia la primera investigación penal.

b) En segundo lugar, el principio de especialidad, que exige la relación de la investigación con un delito concreto, no impide, sin

embargo, el trasvase o cesión de los datos personales recabados en una causa a otro proceso penal, con arreglo al art. 579 bis i. de la LECRIM. Ello queda condicionado a la constatación de la legitimidad de la injerencia en los derechos fundamentales del investigado llevada a cabo en la primera causa, que en este caso es la tramitada en Suiza con la cooperación de la autoridad francesa.

Pero dicha legitimidad para el trasvase de la información, también debería hacerse depender de otra circunstancia relevante, que no es otra que la concurrencia en la segunda causa, es decir, la tramitada en España, de los presupuestos del art. 588 bis a., es decir, la procedencia (necesidad, excepcionalidad, idoneidad, etc.) en el segundo procedimiento de la medida de investigación que conduce a tales datos o informaciones[28]. Si en el segundo proceso, seguido en España, no hubiera sido posible acordar, por ejemplo, la medida de registro remoto del equipo informático para obtener los datos bancarios del acusado, por no tratarse de ninguno de los delitos del art. 588 septies a. de la LECRIM, que no incluye los delitos contra la Hacienda Pública, ¿podría incorporarse la información obtenida con esta medida en la primera causa, sin ponderar si tal medida hubiera sido posible decidirla en el segundo proceso en España? A nuestro entender habría que contestar negativamente a la pregunta, de manera que sería preciso valorar la legitimidad de la adopción de la medida en el proceso de origen y en el segundo proceso. La doble ponderación de la legitimidad de la medida, entendemos debe aplicarse igualmente en el ámbito de la cooperación transfronteriza.

4.3. El principio de proporcionalidad. Las garantías básicas de la cesión y el tratamiento de datos personales en la cooperación judicial penal

A) El at. 4.1 de la Directiva 2016/680, establece los principios relativos al tratamiento de datos personales, de manera que "*..los Estados miembros dispondrán que los datos personales sean:*

---

[28] Problema que apunta COLOMER HERNÁNDEZ, *"La inclinación de la problemática provocada por la transmisión y cesión de datos personales obtenidos en un proceso penal desde el marco normativo comunitaria a la regulación y praxis española",* en VVAA, (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales*...,, op. cit., p. 838.

a) tratados de manera lícita y leal;

b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines;

c) adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados;

d) exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados;

e) conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados;

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas"

La Directiva 2016/680 se refiere pues a un tratamiento de datos personales exactos y actualizados, conservados adecuadamente y tratados de manera segura, en el ámbito de la investigación y enjuiciamiento penal. Un tratamiento lícito, leal y transparente, adecuado y no excesivo, y llevado a cabo únicamente en función de los fines legales preestablecidos (art. 4.1). Ello implica que la medida que conlleve el tratamiento de datos personales debe responder a los siguientes presupuestos.

a) Estar prevista en la ley, resultar necesaria, adecuada, útil, pertinente y proporcionada a los fines de la investigación o del enjuiciamiento de un concreto delito. Así, debe justificarse su pertinencia en cuanto a los fines que se persiguen, y garantizarse que los datos en cuestión no son excesivos para lo que se investiga, ni que se conservarán más tiempo del necesario para los fines que se persiguen, es decir para culminar una investigación o el enjuiciamiento de un delito concreto contra una persona determinada, investigada o encausada.

b) Ser objeto de información al sujeto, especialmente en lo relativo a sus derechos y a los cauces para su defensa, o para hacerlos valer con relación al caso concreto.

c) Y, contar con fines específicos y legítimos, a determinar en el momento de la recopilación u obtención de los datos.

En tal sentido, el art. 8 establece los presupuestos de la licitud del tratamiento de los datos, que son la necesidad en función de los fines de investigación o enjuiciamiento, y la fundamentación de su objetivo, de manera que los Estados deberán prever en sus ordenamientos al menos los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento.

Ahora bien, si esta es la regla general, la Directiva también dispone diversos regímenes de excepciones al elenco de derechos que consagra, y que, no lo olvidemos, vienen referidos a un sospechoso, investigado o encausado en un proceso penal.

Así, el principio rector es que los datos personales se recogen con fines determinados, explícitos y legítimos (art. 4.1), y que fuera del caso concreto debe primar la confidencialidad, impidiendo accesos no autorizados a los datos. Sin embargo, ello no obsta para que estos datos puedan ser usados para otros fines, siempre que no sean incompatibles con los relativos a la investigación y el enjuiciamiento.

En este sentido, el art. 4.2 de la Directiva 2016/680, permite el tratamiento de los datos personales, para fines del art. 1.1 (investigación y enjuiciamiento) distintos de aquel para el que se recogieron, es decir para la investigación o enjuiciamiento de otros hechos delictivos atribuibles a la misma persona o a otra hasta el momento no investigada.

Es decir, un tratamiento de los datos con el mismo fin pero en distinta causa penal. Y ello será posible si el responsable del tratamiento está autorizado, y si es necesario y proporcional con ese otro fin o causa penal. Este es pues el régimen excepcional del principio de especialidad, o régimen de disponibilidad ampliada de la Directiva.

Al respecto, sólo dos apreciaciones. La primera, es relativa a la autoridad que puede utilizar, ceder o transmitir esos datos personales para la investigación o enjuiciamiento de otra causa, que no es aunque debiera serlo, el Juez o el Fiscal, sino el responsable del tratamiento. Dicho responsable deberá valorar la necesidad y proporcionalidad del trasvase de datos al otro proceso, a ese otro "fin no incompatible", así

como la legitimidad de la cesión inicial (el doble control de legitimidad al que nos referíamos en páginas previas).

La segunda, reconocer que la disponibilidad ampliada de la Directiva 2016/680 tiene un ámbito más reducido que el previsto en el art 3.2 de la DM 2008/977. La Directiva de 2008 se refería al uso para otro fin, con el único condicionante de la compatibilidad con el fin para el que se recogieron los datos, mientras el art. 4.2 de la Directiva de 2016, al menos requiere que ese fin debe ser el genérico y único, es decir, la investigación o enjuiciamiento de un delito, aunque en otra causa por hechos o contra personas diferentes. Con ello entendemos que al menos se cierra la puerta a la posibilidad del uso de datos recabados y cedidos en función de una concreta causa criminal a otras vías sancionadoras administrativas o particulares, posibilidad que la redacción del art. 3.2 de la DM de 2008 parecía permitir. En este sentido, se especifica en el Considerando (34) que el tratamiento de datos personales, recopilados para los fines penales previstos en la Directiva, para otros fines diferentes, se regirá en cualquier caso por la Reglamento general 2016/679.

En cualquier caso, la Directiva plantea la necesidad de que los ordenamientos internos cuenten con una base jurídica clara y precisa sobre los objetivos y finalidades del tratamiento de los datos personales, los procedimientos para el mantenimiento de su integridad y confidencialidad, así como los necesarios en orden a su destrucción, con las garantías suficientes en orden a evitar abusos y arbitrariedades.

El tratamiento de los datos personales, en orden a los fines de prevención, detección, investigación y enjuiciamiento, y en su caso ejecución de resoluciones penales, abarca toda operación con datos o conjuntos de datos personales, de forma automatizada o no, entre las que se encuentran la recopilación, registro, organización, estructuración, almacenamiento, adaptación o modificación, recuperación, consulta, utilización, cotejo o combinación, limitación de tratamiento, destrucción y supresión (Considerando 34).

El objeto de la cesión deben ser datos exactos, completos y actualizados, a fin de una eficaz cooperación con datos fiables, actuales, íntegros y exactos, así como de la protección del interesado. Estos principios, recogidos en el art. 4.1, d), e) y f), además se completan en el art. 5, sobre las reglas mínimas en materia de plazos de conservación de

los datos, disponiendo que los Estados miembros fijarán plazos apropiados para la supresión de los datos personales o para una revisión periódica de la necesidad de conservación de los datos personales. Las normas de procedimiento garantizarán el cumplimiento de dichos plazos.

En este punto, el art. 588 bis k. de la LECRIM establece las reglas aplicables sobre destrucción y conservación de registros electrónicos e informáticos utilizados en la medida de investigación. En tal sentido, se prevé el borrado y la eliminación de los registros originales y de las copias conservadas cuando transcurran cinco años desde la ejecución de la pena, su prescripción, el sobreseimiento libre o la sentencia absolutoria firme, siempre que no se estime necesaria la conservación a juicio del tribunal.

Igualmente, el art. 6,2, establece que los Estados miembros dispondrán que las autoridades competentes verifiquen la calidad de los datos, y por tanto adopten todas las medidas razonables para garantizar que los datos personales que sean inexactos, incompletos o que no estén actualizados no se transmitan ni se pongan a disposición de terceros. Para ello, dicha autoridad competente, en la medida en que sea factible, controlará la calidad de los datos personales antes de transmitirlos o ponerlos a disposición de terceros.

B) Obviamente, la transmisión y cesión de datos, a efectos de la cooperación judicial penal, tiene su repercusión fundamental en materia de prueba, en este caso transnacional.

Conviene recordar que el art. 8 de la CDFUE, dispone que el tratamiento de datos personales se realizará de modo leal, para fines concretos, sobre la base del consentimiento del sujeto o, en su caso, en virtud de otro fundamento legal y legítimo como o es la represión, investigación y enjuiciamiento del delito..

Estos principios rectores de finalidad, especialidad y proporcionalidad, ya vistos en páginas anteriores, condicionan la obtención de datos personales y su consiguiente cesión y tratamiento a efectos penales, constituyendo pues los presupuestos habilitantes de las medidas de investigación que inciden o limitan el derecho fundamental a la protección de datos personales.

Partíamos en este punto de un casi vacío normativo en la materia, ante la inaplicación práctica del instrumento que regulaba el exhorto

europeo de obtención de prueba (DM 008/978)[29]. El exhorto no era sino una manifestación del auxilio judicial a través de la transferencia a la autoridad judicial de otro Estado de elementos probatorios que ya se tienen en un causa penal[30].

El estrecho ámbito de aplicación de la DM 2008/978[31], sobre el exhorto europeo de obtención de prueba, destinado a recabar objetos, documentos y datos, pero no a llevar a cabo pruebas transfronterizas, dio lugar a que el instrumento gozase de escaso éxito. Por ello, se vino reclamando un único instrumento sobre cooperación judicial que incluyera la mayor parte de medidas de investigación transfronteriza. Las iniciativas a este respecto dieron lugar a la Directiva 2014/41/CE, del Parlamento Europeo y del Consejo, de 3 de abril de 2014, sobre la OEI[32], que establece la prueba transnacional, en definitiva un auténtico sistema de equivalencia y confianza recíproca para la ejecución de la orden emitida por la autoridad judicial de un Estado, a fin de la obtención de fuentes de prueba a practicar por el Juez de otro Estado.

Evidentemente, como afirma MARTINEZ GARCÍA[33], hay una diferencia esencial entre ambos sistemas de cooperación judicial. El exhorto europeo parte de una prueba, de datos o de una fuente de prueba ya obtenidas por el Estado requerido, y cuya transferencia se pide por el Estado emisor, lo que implica poco más que la asistencia judicial en su concepción más clásica. Sin embargo, la OEI puede suponer una mayor profundización en el principio de reconocimiento mutuo, ya que se pide al Estado requerido la práctica de una medida de investigación y la

---

29 DM 2008/978/JAI, del Consejo, de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de prueba (DO L 350 de 30 de diciembre de 2008).

30 GONZÁLEZ CANO, *"La propuesta de DM relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos",* en VVAA, *La prueba en el espacio de libertad, seguridad y justicia*, Cizur Menor, 2006, pp. 95 a 116.

31 Entre otros, v. AGUILERA MORALES, "*El exhorto europeo de investigación. A las búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas",* en BIMJ, nº 2145, agosto de 2012.

32 DO L 130, de 1 de mayo de 2014.

33 MARTINEZ GARCIA, *La orden europea de investigación. Actos de investigación, ilicitud de prueba y cooperación judicial transfronteriza,* Tirant Lo Blanch, Valencia, 2016, pp. 52 y 53.

obtención de una fuente de prueba a utilizar como material incriminatorio en el Estado emisor.[34]

El mandato de transposición de la Directiva 2014/41, sobre la OEI, se cumple con la modificación de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la UE, operada por la Ley 3/2018, de 11 de junio, que regula la OEI.

Una inicial aproximación a las referencias sobre cesión y protección de datos personales, tanto en la Directiva 2014/41, como en la Ley 23/2018 para su transposición, nos conducen a varias reflexiones.

a) Por una parte, de esencial importancia serán las previsiones sobre la prueba transfronteriza obtenida mediante la emisión y posterior reconocimiento y ejecución de una OEI, sobre todo en lo que hace referencia a la posible denegación de ejecución por ser un medio probatorio de imposible realización en el Estado receptor, o por no venir referido a una causa concreta (principio de especialidad).

Igualmente, serán de máxima importancia las garantías para su obtención, en definitiva la licitud de la misma, en orden a su utilización en el Estado receptor como prueba de cargo suficiente para desvirtuar la presunción de inocencia.

En tal sentido, el art. 14 de la Directiva de 2014 sobre la OEI, prevé el derecho al recurso, al igual que, como veíamos, la Directiva 2016/680 se refiere a los derechos de acceso, rectificación o supresión (arts. 13 a 18).

El art. 189.3 de la Ley 23/2014, disponía respecto al exhorto europeo para obtención de pruebas penales, que la prueba obtenida mediante exhorto producía efectos plenos, sin posibilidad de recurso para controlar las garantías en su obtención. Esta previsión del art. 189.3 de la Ley 23/2014, no atendía a los parámetros de proporcionalidad y defensa que deben regir en esta materia[35] . Téngase presente, como

---

[34] Realmente el art. 1 de la Directiva 2014/41, establece un ámbito de cooperación más amplio, ya que incluye la petición de práctica de actividad probatoria, la obtención de pruebas que ya obren en poder del Estado requerido, e incluso la realización de medidas de aseguramiento de fuentes de prueba.

[35] MARTINEZ GARCÍA, *La orden europea de investigación...,* op. cit., pp. 43 y 44.

apunta BACHMAIER[36], que la norma estaba disponiendo la extensión del reconocimiento mutuo a la admisión de la prueba obtenida en otro Estado, opción del Legislador español que no venía impuesta por la DM y que podía resultar discutible, ya que para establecer una norma de reconocimiento mutuo, no sólo en cuanto a la obtención de la prueba, sino también en materia de admisión de la prueba y valoración de la misma como prueba de cargo, sería imprescindible llevar a cabo la armonización o incluso aproximación normativa necesaria, como diremos más adelante.

b) Por otra parte, y en segundo lugar, la utilización de la OEI, para la obtención de datos personales que obren en Registros de otros Estados miembros, plantea relevantes cuestiones desde el punto de vista del derecho de defensa, y en cuanto a los principios rectores de una medida tal, es decir, la proporcionalidad, la ponderación entre los efectos de la medida y la trascendencia del delito a investigar o enjuiciar, el posible catálogo de delitos en los que utilizar esta medida, así como la idoneidad y la necesidad de la misma.

El Estado emisor de una OEI debe realizar en la propia solicitud y en la resolución que la respalda, un juicio de ponderación sobre la proporcionalidad de la medida que pide, relativo a la especialidad, finalidad, necesidad e idoneidad, en definitiva al cumplimiento de los principios rectores para llevar a cabo toda medida de investigación limitativa de los derechos del art. 18 de la CE (tal y como dispone el art. 588 bis a. de la LECRIM), entre ellas las que impliquen limitación del derecho a la protección de datos.

Así, el art. 6 de la Directiva 2014/41 dispone como condición para la emisión y transmisión de la OEI, la necesidad y proporcionalidad de la misma respecto al procedimiento en el que se va a incorporar la fuente de prueba que se obtenga a partir de la medida de investigación que se solicita, y en relación a los contenidos especificados en el art. 5 (datos

---

[36] BACHAMAIER WINTER, *"El exhorto europeo de obtención de pruebas: análisis normativo"*, en VVAA (dir. y coord. por ARANGUENA FANEGO, DE HOYOS SANCHO y RODRÍGUEZ-MEDEL NIETO), *Reconocimiento mutuo de resoluciones penales en la Unión Europea,* Aranzadi, Navarra, 2015, pp. 516 a 519. Igualmente, MARTINEZ GARCIA, *La orden europea..,* op. cit., pp. 43 y 44.

de la causa, objeto y motivos de la OEI, delitos y hechos enjuiciados y concreta medida pedida).

En el mismo sentido, el art. 20 de la Directiva 2014/41 sobre la OEI, prevé expresamente la protección de los sujetos investigados en orden al tratamiento de datos de carácter personal, en cuanto derecho fundamental del art. 8 de la CDFUE y del art. 16.I del TFUE. En concreto, se dispone que los datos personales obtenidos en virtud de una OEI se procesarán y tratarán de forma leal y transparente, cuando sea necesario y proporcionado para fines compatibles con la prevención, detección, investigación y enjuiciamiento de delitos, la aplicación de sanciones penales y el ejercicio de los derechos de defensa. Igualmente, el art. 20 se remite en orden a los derechos y a la protección del investigado, a la DM 2008/977, ahora entendemos que a la Directiva 2016/680 y por tanto a los principios rectores de la misma que veíamos en páginas previas, y que condicionarán la validez de la recogida, tratamiento y transferencia a efectos probatorios penales de los datos personales.

Estas previsiones deberán aplicarse no sólo en relación con la OEI, por lo que la Ley española de transposición (Ley 3/2018), ha recogido estos principios generales en materia de protección de datos personales de investigados o encausados, no en el articulado referido a la OEI, sino en la DA 5ª de la Ley de reconocimiento mutuo, que dispone que *„los datos de carácter personales obtenidos como consecuencia de la emisión o ejecución de un instrumento de reconocimiento mutuo estarán protegidos de conformidad con lo dispuesto en la normativa europea y española de protección de datos de carácter personal"*.

Más específicamente, el art. 193 de la Ley 23/2014, sobre la utilización en España de los datos personales obtenidos en la ejecución de la orden europea de investigación en otro Estado miembro, dispone que los datos personales obtenidos de la ejecución de una orden europea de investigación sólo podrán ser empleados en los procesos en los que se hubiera acordado esa resolución, en aquellos otros relacionados de manera directa con aquél o excepcionalmente para prevenir una amenaza inmediata y grave para la seguridad pública. Se trata pues de una suerte de transposición del principio de disponibilidad ampliada recogido en la Directiva 2016/680, que tratábamos en páginas anteriores.

Además, el precepto establece que para utilizar con otros fines los datos personales obtenidos, la autoridad española competente deberá recabar el consentimiento de la autoridad del Estado de ejecución o del titular de los datos.

Ello se completa con la previsión de que cuando en un caso concreto así lo requiera la autoridad competente del Estado de ejecución, la autoridad española competente le informará del uso que haga de los datos personales que se hubieran remitido a través de una orden europea de investigación, con excepción de aquéllos obtenidos durante su ejecución en España.

En este sentido es importante resaltar que con arreglo al ordenamiento procesal penal español, las medidas de investigación que impliquen limitaciones de los derechos fundamentales del art. 18 de la CE deben contar con autorización judicial previa a instancia de la Policía Judicial o del MF (arts. 588 bis a. b. y c.). Será el Juez el que realice la ponderación sobre la adecuación de la medida a los principios rectores mencionados (art. 588 bis c.), independientemente de las facultades que en determinados casos ostenta el MF y la Policía Judicial para la obtención de datos previos para elaborar la solicitud de tales medidas (así, el acceso a datos de identificación de usuarios, terminales y dispositivos de conectividad de los arts. 588 ter l. y m.).

c) En tercer lugar, bien es cierto que se ha avanzado considerablemente en el ya citado programa de aproximación normativa en materia de garantías procesales penales de sospechosos e investigados, y fundamentalmente en materia de presunción de inocencia. Sin embargo, la reciente Directiva en esta materia 2016/343, de 9 de marzo de 2016[37], es parca y limitada, con algunas referencias muy genéricas a la carga de la prueba, al derecho al silencio, al derecho a estar presente en el juicio, al recurso, y a la presunción de inocencia. Y desde luego no llega en ningún caso a superar las diferencias entre modelos de investigación y enjuiciamiento en materia de prueba y de obtención de fuentes de prueba, sobre todo si el medio de investigación implica injerencia en los derechos fundamentales.

[37] DO L65, de 11 de marzo de 2016.

En tal sentido, dejamos apuntadas una serie de cuestiones, a nuestro entender muy relevantes, y cuyo tratamiento merece una más amplia investigación.

La primera de estas cuestiones se refiere a si la actividad probatoria objeto de la ejecución de una OEI, y la preconstitución probatoria resultado de la misma, en este caso en orden a datos personales cedidos y tratados, se va a regir por los stándares del TJUE, que deberá determinar si la Directiva 2016/680 se adecúa o no al CEDH y a la CDFUE, y siendo probable que se cuestione de nuevo la preeminencia de estos estándares independientemente de los estándares probatorios de los TC de los Estados.

Y, la segunda cuestión, directamente relacionada con la primera. En caso de prueba transfronteriza relativa a datos personales del investigado o acusado, ¿será necesaria la aproximación normativa en orden al establecimiento de la regla de exclusión como prueba de cargo válida y suficiente? ¿Se reproducirán situaciones como la del Caso *Melloni* o como la del caso *Pupino*, y por tanto la imposiblidad de denegar el reconocimiento mutuo por motivos diferentes a los que derivan de la Directiva en cuestión, como normas mínimas que vinculan a los Estados, aunque sus estándares propios de protección sean superiores? En estos casos ¿prevalecerá la regla de exclusión probatoria que determine el TJUE en materia de prueba ilícita?[38]

La obtención, cesión y tratamiento de datos personales mediante la OEI, y de acuerdo a los principios rectores de la nueva Directiva 2016/680, nos conduce ineludiblemente a reflexionar sobre estas cuestiones de la licitud y la valoración de esta prueba transnacional.

El art. 3 de la Directiva 2014/41, establece que la OEI comprende todas las medidas de investigación que pueden adoptarse en un proceso penal; de manera que la OEI tiene un carácter general y horizontal, tal y como se recoge en el Considerando (8) de la Directiva.

Evidentemente, si bien es verdad que la falta de definición de un concepto de medida de investigación, contribuye a entender que caben todas aquellas que sean necesarias en el Estado de ejecución, también

[38] MARTINEZ GARCIA, "*La orden de investigación europea: las futuras complejidades previsibles en la implementación de la Directiva en España (I)*", en La Ley, nº 106, enero – febrero de 2014.

es cierto que puede ocasionar graves problemas respecto a su valor probatorio, tema fundamental en el proceso penal.

Y es que tanto en este punto, como en materia de reglas de control de legalidad y proporcionalidad, no existe armonización normativa, estableciéndose en cambio un sistema de doble control de estas garantías, tanto en el Estado de emisión de la OEI, imprescindible para después contar con la admisibilidad probatoria, como en el Estado de ejecución, que no supervisa el control en origen, pero atendiendo a su Derecho interno sí que determina la aceptación de la OEI, o bien la sustitución por otra más idónea o menos onerosa, o la denegación (art. 206.5 de la Ley de reconocimiento mutuo).

Este sistema de doble control nos hace pensar que la OEI, más que un mandato de actividad para llevar a la practica una medida de investigación concreta, es un mandato de resultado, con lo cual puede dudarse de su naturaleza como auténtico instrumento de reconocimiento mutuo.

La admisibilidad de la prueba transfronteriza eludiendo este sistema, sólo resultaría posible consiguiendo stándares comunes de proporcionalidad, homogeneización de garantías en las medidas de investigación limitativas de derechos fundamentales, y armonización de reglas de exclusión probatoria.

Mientras ello no sea posible o viable, es imprescindible, por una parte, acudir a un sistema de doble control de admisbilidad en los Estados de emisión y ejecución y, por otra, frente al reconocimiento incondicional del exhorto europeo que se establecía en el anterior art. 189.3 de la Ley de reconocimiento mutuo, aplicar el paradigma de los nuevos arts. 186.1 y 207.1, que condiciona la validez en España de actos de investigación realizados por el Estado de ejecución, al respeto a los principios fundamentales del ordenamiento español así como a las garantías procesales.

5. BIBLIOGRAFÍA

AGUILERA MORALES, *"El exhorto europeo de investigación. A las búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas",* en BIMJ, nº 2145, agosto de 2012.

BACHAMAIER WINTER, *"El exhorto europeo de obtención de pruebas: análisis normativo",* en VVAA (dir. y coord. por ARANGUENA FANEGO, DE HOYOS

SANCHO y RODRÍGUEZ-MEDEL NIETO), *Reconocimiento mutuo de resoluciones penales en la Unión Europea,* Aranzadi, Navarra, 2015.

BAYO DELGADO – GUTIERREZ ZARZA – MICHAEL ALEXANDER, *"Intercambio de información, protección de datos y cooperación judicial penal"*, en VVAA (coord. por GUTIERREZ ZARZA), *Nuevas tecnologías, protección de datos personales y proceso penal,* La Ley, Madrid, 2012.

BLANCO QUINTANA, *"La comunicación de antecedentes penales entre los Estados. El Sistema europeo de información de antecedentes penales"*, en BMJ, 2013.

DE HOYOS SANCHO, *"Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos"*, en VVAA (dir. por ARANGUENA FANEGO), *Espacio europeo de libertad, seguridad y justicia: últimos avances en cooperación judicial penal,* Lex Nova, Valladolid, 2010.

COLOMER HERNÁNDEZ, *"La inclinación de la problemática provocada por la transmisión y cesión de datos personales obtenidos en un proceso penal desde el marco normativo comunitaria a la regulación y praxis española",* en VVAA, (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, Pamplona, 2015.

DREWER - GUTIERREZ ZARZA - MORÁN MARTINEZ, *"Intercambio de información y protección de datos personales en el ámbito de Eurojust, Europol y OLAF",* en VVAA (coord.. por GUTIERREZ ZARZA), *Nuevas tecnologías, protección de datos personales y proceso penal*, La Ley, Madrid, 2012.

ETXEBERRIA GURIDI, *"La protección de datos de ADN en la Unión Europea",* en VVAA (dir. por CABEZUDO BAJO*), Las bases de datos policiales de ADN ¿son una herramienta realmente eficaz en la lucha contra la criminalidad grave nacional y transfronteriza?,* Dykinson, Madrid, 2013.

FIODOROVA, *"La transmisión de información personal y datos personales en la Unión Europea para fines de investigación de delitos",* en VVAA (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, Pamplona, 2015.

FIODOROVA*, "Cesión de datos personales en posesión de Europol",* en VVAA (dir. por COLOMER HERNÁNDEZ), *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios,* Aranzadi, Pamplona, 2017.

FREIXES SANJUAN, *"Protección de datos y globalización. La Convención de Prüm",* en Revista de Derecho Constitucional europeo, nº 7, enero – junio de 2007.

GALÁN MUÑOZ, *"La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea",* en VVAA (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, Pamplona, 2015.

GALÁN MUÑOZ, *"Los nuevos instrumentos de prevención y lucha contra el nuevo terrorismo: malas noticias para la intimidad y otros derechos fundamentales",* en VVAA, *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios,* Aranzadi, Pamplona, 2017.

GÓMEZ COLOMER, *La prueba de ADN en el proceso penal,* Tirant lo Blanch, Valencia, 2014.

GONZÁLEZ CANO, "*Nuevos paradigmas de la cooperación judicial penal en la Unión Europea",* en VVAA (ed. por BARONA VILAR), *Justicia civil y penal en la era global*, Tirant lo Blanch, Valencia, 2017.

GONZÁLEZ CANO, *"Algunas reflexiones sobre protección de datos personales, proceso penal y cooperación judicial penal en la Unión Europea",* en Cuadernos digitales de formación del Consejo General del Poder Judicial, Nº 29- 2012.

GONZÁLEZ CANO, *"Cesión y tratamiento de datos personales, principio de disponibilidad y cooperación judicial penal en la Unión Europea",* en VVAA Dir. por COLOMER HERNÁNDEZ), *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios*, Aranzadi, Pamplona, 2017.

GONZÁLEZ CANO, *"La propuesta de DM relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos",* en VVAA, La prueba en el espacio de libertad, seguridad y justicia, Cizur Menor, 2006.

GONZÁLEZ CANO *"Garantías del investigado y acusado en orden a la obtención, cesión y tratamiento de datos personales en el proceso penal. a propósito de la Directiva (UE) 2016/680 y su impacto en materia de prueba penal",* en VVAA (dir. por GONZÁLEZ CANO), Orden europea de investigación y prueba transfronteriza en la Unión Europea, Tirant lo Blanch, Valencia, 2019.

GONZÁLEZ PASCUAL, *"El TJUE como garante de los derechos de la UE a la luz de la Sentencia Digital Right Ireland",* en Revista de Derecho Comunitario Europeo, nº 49, 2014.

MARTINEZ GARCIA, *La orden europea de investigación. Actos de investigación, ilicitud de prueba y cooperación judicial transfronteriza,* Tirant Lo Blanch, Valencia, 2016.

MARTINEZ GARCIA, "*La orden de investigación europea: las futuras complejidades previsibles en la implementación de la Directiva en España (I)*", en La Ley, nº 106, enero – febrero de 2014.

PARIENTE DE PRADA, *El Espacio de libertad, seguridad y justicia: Schenguen y protección de datos,* Aranzadi, Cizur Menor, 2013.

RICHARD GONZÁLEZ, *"La conservación y utilización de datos de las comunicaciones en la investigación criminal. Problemas que resultan de la aplicación de la doctrina del TJUE"*, en VVAA (dir. por JIMÉNEZ CONDE*), Adaptación del Derecho Procesal español a la normativa europea y su interpretación por los tribunales*, Tirant lo Blanch, 2018,

SOLAR CLAVO, *"La doble vía europea en protección de datos",* en La Ley, nº 2832, 2012.

VERVAELE, *"¿La asociación organizada terrorista y sus actos anticipativos: un derecho penal y política criminal sin límites?",* en VVAA (dir. por GONZALEZ CANO), *Integración europea y justicia penal,* Tirant lo Blanch, Colección Alternativas, Valencia, 2018.

VILLARINO MARZO, *"La Unión Europea ante los retos de la era digital. La reforma de la política europea de protección de datos",* en VVAA (dir. por PASCUA MATEO), *Derecho de la Unión Europea y Tratado de Lisboa,* Civitas, Madrid, 2013.

Informações adicionais e declarações dos autores (*integridade científica*)

Declaração de conflito de interesses (conflict of interest declaration): a autora confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

Declaração de ineditismo e originalidade (declaration of originality): a autora assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 10/09/2019
- Retorno rodada de correções: 21/09/2019
- *Autores convidados*

http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies - custom-1

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editoras-associadas: 2 (CC e BC)

COMO CITAR ESTE ARTIGO:

GONZÁLEZ CANO, Mª Isabel. Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1331-1384, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.279

L'archiviazione dei dati genetici a fini di giustizia penale: gli interessi in gioco, le prescrizioni europee, le soluzioni adottate dal legislatore italiano

Storage of genetic data for criminal justice purposes: interests at stake, European regulations, solutions adopted by Italian lawmakers

Arquivamento de dados genéticos com finalidades penais: interesses em jogo, regulações europeias e soluções adotadas pelo legislador italiano

Chiara Gabrielli[1]

Università degli Studi di Urbino Carlo Bo/Italia
chiara.gabrielli@uniurb.it
http://orcid.org/0000-003-4605-2319

Abstract: Dotarsi di un *database* dei dati genetici a fini di giustizia penale rappresenta per qualsiasi ordinamento una sfida ineludibile, ma di particolare delicatezza. Ineludibile, perché immagazzinare profili del dna appartenenti a una determinata platea soggettiva in vista della comparazione automatizzata mediante procedure informatiche significa mettere a disposizione degli inquirenti risorse di innegabile rilevanza probatoria. Particolarmente delicata, in quanto dalle scelte che governano acquisizione, conservazione e consultazione di dati geneticamente significativi dipende l'impatto che la "biologizzazione della sicurezza" è destinata a produrre sulla c.d. *informational privacy*, intesa come diritto dell'individuo al controllo delle informazioni riguardanti la propria sfera personale, tutelata dall'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. In Italia, la banca dati del dna è divenuta operativa soltanto di recente, al termine di un faticoso percorso legislativo. Il contributo si propone di

[1] Ricercatrice di Diritto processuale penale.

analizzare le scelte tecniche e valoriali operate dalla legge n. 85 del 2009 e dei provvedimenti di attuazione, verificandone la capacità di assicurare un bilanciamento tra gli interessi in contrasto conforme ai parametri di ragionevolezza e proporzionalità e la sintonia con le indicazioni della giurisprudenza della Corte europea dei diritti dell'uomo. Soltanto a queste condizioni il sacrificio richiesto alla "*privacy* genetica" per il perseguimento degli scopi di giustizia penale può risultare culturalmente e socialmente accettabile, oltre che giuridicamente legittimo. Non c'è dubbio, infatti, che la domanda collettiva di sicurezza sia divenuta progressivamente più insistente, anche per il diffondersi del fenomeno terroristico; altrettanto innegabilmente, però, si è acuita la sensibilità collettiva verso le differenti declinazioni della riservatezza personale, in special modo nei confronti di un patrimonio genetico ormai percepito come "marchio" dell'individualità soggettiva. Nessun ordinamento moderno, dunque, può sottrarsi al compito di rendere la tecnologia alleata della *privacy* tanto quanto della giustizia penale.

Parole-chiave: Dati genetici; banca dati del dna; sicurezza collettiva; riservatezza; ingerenza nella vita privata e familiare.

Abstract: *For any legal system, having a genetic database for the purposes of criminal justice represents an unavoidable but particularly delicate challenge. Unavoidable, because storing DNA profiles that belong to a given subjective population for computer comparison means providing investigators with resources of undeniable probative value. Particularly delicate, as the choices that determine the acquisition, conservation and consultation of genetically significant data generate the impact of the "biologisation of security" on so-called informational privacy, namely the right of the individual to check information that regards his/her personal sphere, defined by article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. In Italy, the DNA database has recently become operational, following a laborious legislative procedure. This contribution sets out to analyse the technical and value-related bases for law no. 85 of 2009 and the provisions for its introduction. It also proposes to assess this law's capacity to ensure an adequate balance between contrasting interests that keep within the parameters of reasonableness and proportionality, as well as being in congruence with the jurisprudence of the European Court of Human Rights. It is only on these conditions that the sacrifice required of "genetic privacy" for the pursuit of the aims of criminal justice could be deemed culturally*

and socially acceptable, as well as juridically legitimate. Indeed, there is no doubt that the collective demand for security has become progressively more insistent, also in view of the growth of terrorism. Just as undeniable, however, is the public's growing sensitivity towards the various aspects of personal confidentiality, especially regarding a genetic heritage that is now seen as a mark of subjective individuality. No modern law system can thus avoid the task of making technology an ally of privacy, especially in the ambit of criminal justice.

Keywords: *genetic data; genetic forensic database; public security; privacy; interference in private and family life.*

Resumo: *Criar um banco de dados genéticos com finalidades penais representa para qualquer ordenamento um desafio inevitável e, contemporaneamente, muito delicado. É inevitável porque armazenar perfis de DNA pertencentes a um determinado grupo de sujeitos para realizar uma comparação automatizada mediante procedimentos informáticos significa disponibilizar aos órgãos investigativos informações de inegável relevância probatória. Particularmente delicada pois em razão das escolhas que governam a colheita, conservação e consulta de dados genéticos relevantes depende o impacto que a "biologização da segurança" finda por produzir em relação à denominada informational privacy, ou seja, o direito do indivíduo ao controle das informações relativas à própria esfera pessoal, tutelado pelo art. 8 da Convenção Europeia dos direitos humanos. Na Itália, o banco de dados do DNA tornou-se operativo somente recentemente, após um percurso legislativo demasiadamente tormentoso. Neste artigo serão analisadas as escolhas técnicas e valorativas efetuadas pela Lei n. 85 de 2009 e pelas regulamentações de atuação, verificando a sua capacidade de assegurar um balanceamento entre os interesses em jogo em contraste conforme os parâmetros de razoabilidade e proporcionalidade e a sintonia com as indicações da jurisprudência do Tribunal europeu dos direitos humanos. Somente se atendidas tais condições, o sacrifício imposto à "privacidade genética" para o alcance dos objetivos de justiça penal pode ser considerado culturalmente e socialmente aceitável, além de juridicamente legítimo. De fato, não há dúvidas de que o clamor coletivo por segurança se tornou progressivamente mais insistente, especialmente pela difusão do fenômeno do terrorismo. Não obstante, é também inegável que a sensibilidade coletiva se tornou mais atenta em relação às diferentes declinações na privacidade pessoal, e, em particular, ao patrimônio genético agora percebido como marca da individualidade subjetiva. Nenhum ordenamento moderno, portanto, pode subtrair-se*

à tarefa de tornar a tecnologia uma aliada da privacidade tanto quanto da justiça penal.

Palavras-chave: *Dados genéticos; banco de dados de DNA; segurança coletiva; privacidade; ingerência na vida privada e familiar.*

1. Una sfida impegnativa, ma non eludibile

"Ogni criminale lascia una traccia di sé sulla scena del crimine", teorizzava già agli inizi del '900 il criminologo francese Edmond Locard, direttore a Lione del primo laboratorio di polizia scientifica, intuendo l'inevitabile interscambio che si realizza, in presenza di alcune condotte criminose, tra l'autore del reato, la vittima e il luogo dell'evento. Dalla traccia biologica lasciata da un soggetto è possibile estrarre un'impronta genetica, che lo connota in modo esclusivo: la rivoluzionaria scoperta fu compiuta nel 1984 da Alec J. Jeffreys, genetista dell'Università di Leicester. Dunque, quando si registra una corrispondenza tra la stringa del dna estratta dal campione biologico prelevato a un determinato soggetto e il profilo genetico ricavato da un reperto organico rinvenuto sulla scena del crimine, addosso alla vittima del reato, sulla superficie dell'arma del delitto, si può ragionevolmente ritenere che tale soggetto si sia recato in quel luogo, sia entrato in relazione con la persona offesa, sia stato a contatto con l'arma del delitto[2]. Il che non significa rispondere «all'ultima

[2] «Una sola differenza è sufficiente per escludere che due profili vengano dalla stessa persona; se invece le sequenze sono sovrapponibili, si può concludere che risalgono ad un unico soggetto; concettualmente si tratta d'una valutazione probabilistica (infatti è necessario calcolare, attraverso modelli matematico-statistici, con quale frequenza determinati geni ricorrano nell'ambito della popolazione di riferimento); ma la probabilità può essere talmente alta da

abduzione, quella che permette di attribuire il reato a un soggetto»[3], ma dimostrare una circostanza che potrebbe risultare risolutiva per gli esiti dell'accertamento penale.

Considerata la relativa facilità con cui nell'era dell'informatica i dati genetici possono essere gestiti e catalogati mediante *software*, non ha tardato a farsi strada nei diversi Paesi, a cominciare dal Regno Unito[4], l'idea di immagazzinare preventivamente in una banca dati nazionale i profili del dna appartenenti a una "qualificata" platea soggettiva, così da rendere disponibili a fini di giustizia penale – «in modo continuativo e indipendente da questa o quella indagine, da questo o quel procedimento in corso»[5] – informazioni rapidamente confrontabili, attraverso procedure di comparazione automatizzata.

Sul versante dell'identificazione personale, la corrispondenza riscontrata tra il profilo relativo a un indiziato la cui identità anagrafica sia incerta e uno dei profili custoditi nel *database* consentirà di stabilire le generalità esatte dell'interessato. Sul versante probatorio, il *match*

---

rasentare la certezza» (CAMON, Alberto, *La disciplina delle indagini genetiche*, in *Cass. pen*., 2014, p. 1427).

3 Così FASSONE, Elvio, *Le scienze come ausilio nella ricerca del fatto e nel giudizio di valore*, in DE CATALDO NEUBURGER, Luisa (a cura di), *La prova scientifica nel processo penale*, Cedam, 2007, p. 247, il quale esemplifica: «se la scienza dice che quella impronta appartiene a Tizio, questo ci autorizza a ritenere che Tizio ha toccato quell'oggetto, non che Tizio abbia commesso il furto in quell'appartamento, nel quale può avere avuto accesso per legittime ragioni. Così per la traccia rinvenuta, che, analizzata quanto al DNA, conduce a Caio». La prova del dna dovrebbe essere correttamente ritenuta «una prova indiziaria a matrice statistica», sintetizza LUPARIA, Luca, *Dati genetici e cultura processuale: un futuro ancora da comporre*, in MARAFIOTI, Luca, LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Giuffrè, 2010, p. 348, e subire «il filtro dei necessari riscontri e l'operatività della regola di giudizio dell'"oltre ogni ragionevole dubbio"» (PRESUTTI, Adonella, *L'acquisizione forzosa dei dati genetici tra adempimenti internazionali e impegni costituzionali*, in *Riv. it. dir. proc. e pen*., 2010, p. 548).

4 Paese in cui la banca dati dei profili del dna esiste già dal 1995.

5 GENNARI, Giuseppe, *La istituzione della banca dati del Dna ad uso forense: dalla* privacy *alla sicurezza*, in SCARCELLA, Alessio (a cura di), *Prelievo del DNA e banca dati nazionale*, Cedam, 2009, p. 71. Sui vantaggi apportati da tale archivio all'attività inquirente v. anche le riflessioni di ORLANDI, Renzo, PAPPALARDO, Giuseppe, *L'indagine genetica nel processo penale germanico. Osservazioni su una recente riforma*, in *Dir. proc. pen*., 1999, p. 767.

registrato tra un profilo "anonimo" rinvenuto sul luogo del reato e uno dei profili presenti in archivio accrediterà come estremamente probabile il collegamento tra il soggetto cui questo appartiene e l'episodio criminoso; nel caso in cui si tratti della persona sottoposta alle indagini, l'esito del riscontro comparativo rafforzerà il compendio indiziario a suo carico, ferma restando l'esigenza di «inserire sempre la prova del DNA in un più ampio quadro critico di supporto e riscontro, onde evitare inammissibili errori»[6]; ove il profilo risulti appartenere ad un differente soggetto, allontanerà i sospetti dall'indagato e suggerirà nuove prospettive di investigazione da approfondire. Infine, qualora gli inquirenti stiano procedendo contro ignoti, l'abbinamento tra i profili farà finalmente emergere una direzione soggettiva di indagine.

Conservando nell'archivio anche i profili genetici "anonimi", estratti nel corso di un procedimento penale da reperti rinvenuti sulla scena del crimine, si schiudono ulteriori prospettive: inchieste penali rimaste senza esito potrebbero essere riaperte nel caso in cui, immettendo il profilo estratto dal campione di un certo soggetto nella banca dati, si registrasse una corrispondenza con uno dei profili "muti" che vi sono custoditi; spunti investigativi potrebbero emergere anche dal *match* tra due profili "anonimi": diversi episodi criminosi diverrebbero, infatti, plausibilmente attribuibili al medesimo autore.

Essendo impensabile che gli inquirenti rinuncino ad avvalersi delle preziose risorse offerte dalla genetica forense, quell'ordinamento che non si faccia carico di disciplinare l'acquisizione e la conservazione dei profili del dna a fini di giustizia penale mostrerebbe una preoccupante inconsapevolezza. Consegnare improvvidamente la gestione di tali fasi all'anarchia della prassi significherebbe, infatti, favorire disomogenee modalità di acquisizione di campioni e reperti biologici, differenti tecniche di analisi degli stessi ai fini della tipizzazione dei profili e *standard* di sicurezza dei dati non uniformi; ne risentirà, inevitabilmente, la possibilità di esercitare un controllo adeguato sia sull'affidabilità delle prime sia

[6] MARAFIOTI, Luca, *Le banche dati del dna. Una nuova frontiera investigativa nel trattato di Prüm*, in MARAFIOTI, Luca-LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Giuffrè, 2010, p. 8.

sull'efficienza dei secondi[7]; d'altra parte, la frammentazione territoriale degli archivi permetterà unicamente una comparazione "parcellizzata" e quindi parziale, pregiudicando anche le *chance* di cooperazione giudiziaria con gli altri Stati.

Per queste ragioni, la creazione di un'anagrafe nazionale "centralizzata" dei dati genetici a scopi di giustizia penale, disciplinata da un preciso statuto giuridico e organizzata mediante le più efficaci strumentazioni tecnologiche, è compito al quale nessun ordinamento, a qualsiasi latitudine, sembra potersi sottrarre. Si tratta, intuibilmente, di una sfida di notevole complessità. Impone al legislatore di misurarsi con un contesto normativo tendenzialmente "multilivello", in cui convivono, al di là delle differenze geografiche, fonti internazionali, previsioni pattizie, prescrizioni costituzionali, disposizioni in tema di *privacy*, norme processuali. Presuppone, inoltre, il dominio di categorie e di nozioni appartenenti ai territori, meno familiari rispetto a quelli giuridici, della genetica forense e della tecnologia: adeguate conoscenze scientifiche, ricavate dai documenti elaborati dalle più accreditate organizzazioni di esperti della materia[8], sono essenziali per distinguere quale *res* geneticamente rilevante (o sua porzione) sia necessario conservare a fini di identificazione e quale, invece, essendo superflua, non debba essere archiviata[9]; come pure, aggiornate nozioni di genetica forense sono indispensabili al legislatore per rendersi conto di quali ulteriori informazioni, non necessarie a fini identificativi, possa fornire la *res*

---

[7] Aspetti problematici che non hanno impedito alla giurisprudenza di ritenere utilizzabile, «in mancanza della violazione di un divieto di legge, l'accertamento sull'identità dell'indagato compiuto mediante ricorso ai dati relativi al DNA contenuti in un archivio informatico che la polizia giudiziaria abbia istituito prescindendo dalle cautele previste dal codice della *privacy*» (Cass., sez. V, 5 febbraio 2007, Vulicevic ed al., in *CED Cass*., n. 235969).

[8] Ad esempio, il documento "*Dna Data management rewiew and recommendations*" elaborato dall'*ENFSI DNA Working Group*, organizzazione internazionale che riunisce esperti di scienze forensi. Per una sintesi dei suoi contenuti, in rapporto alle scelte del legislatore italiano, v. LAGO, Giampietro, *Banche dati DNA: raccomandazioni internazionali, studio comparato con la Legge 85/2009*, in *Giust. pen*., 2010, p. 142 ss.

[9] «Uno Stato democratico è anche quello che si caratterizza per sobrietà informativa», afferma condivisibilmente RODOTÀ, Stefano, *Difendere i cittadini dagli abusi della scienza*, in *La Repubblica*, 6 gennaio 1999.

custodita nel *database*, così da poter valutare il livello di protezione di cui la stessa deve essere proporzionalmente circondata.

Inoltre, si tratta di una sfida che nessun legislatore avveduto può ritenere di aver vinto in modo definitivo, una volta per tutte. Rispetto alle disposizioni che governano altri settori, la disciplina in questione va incontro fatalmente a un'obsolescenza più rapida; un legislatore accorto dovrebbe perciò mettere in conto periodiche "revisioni" dell'assetto normativo, così da adeguare strumenti e regole ai progressi sia della genetica forense (ad esempio, la messa a punto di più affidabili metodologie di analisi) sia della tecnologia (ad esempio, la sperimentazione di più sofisticate soluzioni informatiche, capaci di assicurare un incremento delle protezione contro illegittimi accessi all'archivio), come pure a non improbabili mutamenti della sensibilità collettiva.

Per tenere meglio il passo dell'evoluzione scientifica, la definizione degli aspetti squisitamente tecnici potrebbe essere affidata a fonti regolamentari, che si prestano ad interventi di modifica più agevoli rispetto alle norme di legge, perché sottratte al confronto parlamentare[10]. I nodi valoriali della materia vanno tuttavia sciolti in sede legislativa; ben lontane dal rappresentare questioni di rilevanza settoriale, le scelte che governano acquisizione, conservazione e consultazione dei dati geneticamente significativi declinano lo storico antagonismo tra sicurezza collettiva e libertà individuali[11], definendo l'impatto che la «biologizzazione della sicurezza»[12] è destinata a produrre sulla c.d.

---

[10] In argomento v. SIGNORATO, Silvia, *Il trattamento dei dati personali per fini di prevenzione e repressione penale*, in *Riv. dir. proc*., 2015, p. 1492 ss.

[11] Ne appariva consapevole, già agli inizi degli anni Novanta, il Comitato dei ministri del Consiglio d'Europa: nel Preambolo della Raccomandazione (92)1 sottolineava i «benefici apportati alla giustizia penale dalle tecniche di analisi del Dna», ma avvertiva lucidamente, altresì, l'esigenza che il loro impiego tenesse «pienamente conto di principi fondamentali quali la dignità propria di ciascuna persona ed il rispetto del corpo umano, il diritto di difesa ed il principio di proporzionalità». Sul «pionieristico (...) apporto del Consiglio d'Europa in tema di tutela dei dati personali, prima, e della prova genetica e banche dati del DNA, poi» v. ALLEGREZZA, Silvia, *Prova scientifica e dimensione europea*, in CANZIO, Giovanni, LUPARIA, Luca (a cura di), *Prova scientifica e processo penale*, Giuffrè, 2018, p. 125.

[12] L'efficace espressione indica «una politica pubblica che fonda il suo operare sull'analisi del DNA» (SCAFFARDI, Lucia, *Giustizia genetica e tutela della persona*, Cedam, 2017, p. 256).

informational privacy, intesa come diritto dell'individuo al controllo delle informazioni riguardanti la propria sfera personale.

Dalla capacità dell'ordinamento di contenere tale impatto entro limiti ragionevoli, peraltro, dipenderà anche la possibilità che il sacrificio richiesto alla "*privacy* genetica" a scopi penali risulti culturalmente e socialmente accettabile, oltre che legittimo. Non c'è dubbio che la domanda collettiva di sicurezza sia divenuta oggi più insistente, anche per il diffondersi del fenomeno terroristico; altrettanto innegabilmente, però, si è acuita la sensibilità verso le variegate espressioni della riservatezza personale, in speciale modo nei confronti di un patrimonio genetico ormai percepito come «il marchio dell'individualità soggettiva»[13]. Al soddisfacimento di entrambe queste istanze – di sicurezza collettiva e di sicurezza dei dati individuali – può certamente contribuire l'evoluzione della tecnologia, alleata preziosa della riservatezza non meno che della giustizia penale. Un ordinamento che opportunamente si avvale di sofisticati *software* che consentono la comparazione automatizzata di un profilo genetico anonimo con la totalità dei profili immessi nella banca dati, facendone emergere l'eventuale corrispondenza in tempi estremamente rapidi, dovrà anche farsi carico di organizzare la "messa in sicurezza" dei dati genetici, ricorrendo alle più avanzate risorse tecnologiche e informatiche disponibili.

2. L'esperienza italiana

Da tempo, per gli ordinamenti dei Paesi aderenti all'Unione europea, dotarsi di strutture idonee ad archiviare dati genetici rappresenta un obbligo giuridicamente ineludibile. Se la Risoluzione del 9 giugno 1997 sullo scambio dei risultati di analisi del dna invitava gli Stati membri dell'Unione europea «a prevedere la costituzione di banche dati nazionali», auspicabilmente caratterizzate da *standard* uniformi, la Decisione 2008/615/GAI del 23 giugno 2008, recependo i contenuti del

[13] DAL MIGLIO, Chiara, GENTILOMO, Andrea, PICCININI Andrea, D'AURIA, Luca, *Dal prelievo coattivo alla banca dati dei profili genetici: l'ennesima incompiuta*, in *Riv. it. dir. med. leg.*, 2007, p. 85.

Trattato di Prüm[14], li obbligava a «creare e gestire schedari nazionali di analisi del DNA per le indagini penali» e ad assicurare reciproci «diritti di accesso» agli stessi, mediante procedure automatizzate di consultazione e di raffronto attivabili dai punti di contatto nazionali dei Paesi membri. Adempimenti necessari a rafforzare quello scambio di informazioni genetiche tra Stati che la c.d. decisione Prüm del 2008 individua come tassello di «fondamentale importanza» per una efficace cooperazione internazionale in materia di giustizia penale.

Pur avendo espresso già nel 2006, tramite il Ministro dell'interno, l'intenzione di aderire al Trattato di Prüm, l'Italia ha recepito tali sollecitazioni con sensibile ritardo: si è dovuto attendere fino a giugno 2009 perché fosse approvata la «prima legge organica sulla acquisizione e il trattamento della bioinformazione genetica a fini forensi»[15]. Il protrarsi dell'inerzia legislativa in materia aveva suscitato l'intervento preoccupato del Garante per la protezione dei dati personali, convinto dell'«urgenza di disciplinare organicamente», con riguardo all'acquisizione dei dati genetici per finalità di accertamento e di repressione dei reati, «competenze, procedure e modalità di tutela degli interessati»[16]. Sullo sfondo si avvertiva la preoccupazione che la perdurante lacuna normativa avrebbe non solo compromesso le *chance* di cooperazione giudiziaria con gli altri Stati, ma anche incentivato il diffondersi di archivi "artigianali", allestiti dalle forze di polizia al di fuori di qualsiasi cornice normativa[17] e perciò caratterizzati «da statuto giuridico incerto e da garanzie a contorni sfumati»[18].

---

[14] Stipulato il 27 maggio 2005 tra Belgio, Germania, Spagna, Francia, Lussemburgo, Paesi Bassi e Austria.

[15] GENNARI, Giuseppe, *Bioinformazione e indagini penali: la l. n. 85 del 30 giugno 2009*, in *Resp. civ. e prev.*, 2009, p. 2630.

[16] *Segnalazione al Parlamento e al Governo sulla disciplina delle banche dati del dna a fini di giustizia, 19 settembre 2007*, in *Bollettino* n. 86 del settembre 2007.

[17] La realtà di un archivio di profili genetici presso il Reparto investigazioni scientifiche (RIS) di Parma era emersa nel corso di un'inchiesta penale per furto, rendendo necessario l'intervento del Garante per la protezione dei dati personali al fine di imporre minime misure di sicurezza. Per una dettagliata descrizione della vicenda v. GENNARI, Giuseppe, *Genetica forense e codice della* privacy*: riflessioni su vecchie e nuove banche dati*, in *Resp. civ. e prev.*, 2011, p. 1184 ss.

[18] DAL MIGLIO, Chiara, GENTILOMO, Andrea, PICCININI, Andrea, D'AURIA, Luca, *Dal prelievo coattivo alla banca dati dei profili genetici: l'ennesima*

La legge n. 85 del 2009 di ratifica del Trattato di Prüm ha istituito la banca dati nazionale del dna e il laboratorio centrale, disciplinandone la fisionomia; numerosi aspetti, decisivi per il funzionamento delle due strutture, erano tuttavia demandati a successivi regolamenti di attuazione[19].

La gestazione normativa si è rivelata molto più lunga di quanto pronosticato dal legislatore, forse con eccessivo ottimismo[20]: il regolamento attuativo, contenente «indicazioni cogenti in termini di qualità analitica, tracciabilità, interpretazione»[21], ha visto la luce soltanto nel 2016[22], rinviando a sua volta, per diverse questioni operative, ad ulteriori provvedimenti, che il Ministro dell'interno avrebbe dovuto adottare di

---

incompiuta, cit., p. 86. Rileva tuttavia «l'ambiguità» della disciplina del 2009, «con riferimento alla sorte degli archivi genetici non ufficiali che sembra siano destinati a convivere con la Banca nazionale del dna», FELICIONI, Paola, *DNA e Banche dati europee*, in AA. VV., *Investigazioni e prove transnazionali*, Giuffrè, 2017, p. 200.

19 Soluzione non implausibile nell'ottica di facilitare l'adeguamento all'evoluzione della genetica forense, rendendo più agevoli le «modifiche delle norme regolamentari che dovessero risultare non in linea con i nuovi standard tecnico-scientifici» (SCOLLO, Giancarlo, *La disciplina attuativa della banca dati del dna e del laboratorio centrale*, in MARAFIOTI, Luca, LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Giuffrè, 2010, p. 165). Perplessità sul rinvio alla fonte regolamentare sono espresse dalla dottrina giuridica: per tutti, ORLANDI, Renzo, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen*., 2014, p. 1155; SANTOSUOSSO, Amedeo, COLUSSI, Ilaria Anna, *La banca dati del DNA: questioni in tema di alimentazione, trattamento e accesso, presupposti, cancellazione e tempi di conservazione (artt. 5-15 l. n. 85/09)*, in *Pol. dir*., 2011, p. 457.

20 La disciplina di attuazione avrebbe dovuto essere emanata entro quattro mesi dall'entrata in vigore della legge n. 85 del 2009, su proposta del Ministro della giustizia e del Ministro dell'interno, e previa interlocuzione con il Garante per la protezione dei dati personali e il presidente del Comitato nazionale per la biosicurezza e le biotecnologie, chiamati a fornire un parere sul relativo schema.

21 RICCI, Ugo, *Un lampo di consapevolezza nella normativa italiana: il DNA oltre la suggestione e il mito*, in *Dir. pen. proc*., 2016, p. 753.

22 Si tratta del *Regolamento recante disposizioni di attuazione della legge 30 giugno 2009, n. 85, concernente l'istituzione della banca dati nazionale del DNA e del laboratorio centrale per la banca dati nazionale del DNA, ai sensi dell'articolo 16 della legge n. 85 del 2009*, adottato con d.P.R. 7 aprile 2016, n. 87, in *G.U*., 26 maggio 2016, n. 122.

concerto con il Ministro della giustizia[23]. Ora che il "mosaico normativo" si è finalmente completato, consentendo alla struttura di divenire operativa[24], è possibile analizzarne le opzioni qualificanti in rapporto ai principali plessi problematici posti dall'accantonamento dei dati genetici.

3. *Res* conservate e presidi di sicurezza

Campione biologico e profilo del dna si distinguono per un differente potenziale informativo, che si riflette sulle implicazioni connesse alla loro conservazione[25]. Essendo un «codice alfanumerico» relativo alla «parte non codificante di un campione di dna umano analizzato»[26], il profilo del dna non consente di ricostruire le

---

[23] Con decreto del Ministro dell'interno del 12 maggio 2017 sono state definite le modalità di cancellazione dei profili del dna, di distruzione dei campioni biologici, di immissione e aggiornamento dei dati necessari ai fini della determinazione dei tempi di conservazione dei medesimi profili del dna; con decreto del Ministro dell'interno dell'8 novembre 2016 sono state disciplinate le «procedure per il trattamento dei dati, da parte della banca dati del DNA e del laboratorio centrale per la banca dati nazionale del DNA, e per la trasmissione del profilo del DNA da parte dei laboratori di istituzioni di elevata specializzazione, in attuazione degli articoli 3, 4 e 6 del decreto del Presidente della Repubblica 7 aprile 2016, n. 87».

[24] Un primo bilancio dei risultati finora ottenuti e dei progressi nell'implementazione della struttura si rinviene nell'intervista di Giusi Fasano a Renato Biondo, dirigente della Polizia di Stato e direttore della banca dati nazionale del dna (*Quella banca dati di pochi DNA*, in *Corriere della Sera*, 26 aprile 2019).

[25] Sulla differenza tra la conservazione delle impronte digitali da un lato, dei campioni di materiale biologico e dei profili genetici dall'altro, in conseguenza delle maggiori potenzialità informative proprie di queste ultime due categorie di dati, v. Corte eur. dir. uomo, 7 dicembre 2006, Van der Velden c. Paesi Bassi. Sul maggiore «grado di criticità» della conservazione dei campioni rispetto al «trattamento dei profili» v. le osservazioni di COCITO, Andrea, *Parametri internazionali e affidabilità dei laboratori nelle analisi dei reperti e campioni*, in MARAFIOTI, Luca, LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Giuffrè, 2010, p. 99.

[26] La definizione contenuta nell'art. 2 lett. *v*) d.P.R. n. 87 del 2016 ricalca quella formulata dall'art. 2 lett. *c*) della Decisione 2008/616/GAI adottata il 23 giugno 2008 dal Consiglio dell'Unione europea, perfezionando così la meno completa previsione dell'art. 11 comma 3 legge n. 85 del 2009 («i sistemi di analisi sono applicati esclusivamente alle sequenze del DNA che non consentono la identificazione delle patologie da cui può essere affetto l'interessato»).

caratteristiche fisiche del soggetto cui appartiene, ad eccezione del sesso, né i suoi tratti comportamentali[27]. Il campione biologico possiede, invece, potenzialità informative che oltrepassano quelle legate all'identificazione, evidenziando, ad esempio, patologie, esistenti o non ancora insorte, con conseguenti pericoli, nel caso di un'incontrollata divulgazione, di discriminazioni sul piano sociale ed economico, come pure di pregiudizi alla vita lavorativa e alle relazioni interpersonali[28].

In considerazione di attitudini informative così marcate, la scelta legislativa di conservare anche i campioni biologici, diversamente da quanto avviene in altri ordinamenti[29], ha suscitato perplessità; se per qualcuno il loro "stoccaggio" si può spiegare con la «possibilità di effettuare nuove analisi, magari a richiesta della difesa ed in considerazione dei progressi della scienza»[30], secondo altri comporta «un rischio di violazione

---

[27] RICCI, Ugo, PREVIDERÈ, Carlo, FATTORINI, Paolo, CORRADI, Fabio, *La prova del dna per la ricerca della verità*, Giuffrè, 2006, p. 30 ss. Peraltro, la valutazione delle attitudini informative degli stessi profili non è concetto "statico": come ricordato dal Garante europeo della protezione dei dati nel Parere del 21 luglio 2007, «occorre tener conto anche dei progressi scientifici: quello che in un dato momento è considerato un profilo di DNA "innocuo", potrebbe rivelare successivamente molte più informazioni di quanto non sia prevedibile e necessario». Come osserva SALSI, Giancarlo, *La Banca Dati del DNA. Indagini genetiche e problematiche giuridiche*, Clueb, 2012, p. 155, «quelle che definiamo oggi regioni non codificanti lo sono solamente nella misura in cui non siamo ancora riusciti a decifrarle».

[28] «Il profilo genetico esprime una quantità di informazioni molto ridotta rispetto a quella ricavabile da un campione biologico», il quale «consente di ottenere ampie conoscenze su di una persona in punto di malattie e di caratteristiche ereditarie» (TONINI, Paolo, *Accertamento del fatto e informazioni genetiche: un difficile bilanciamento*, in *Dir. pen. proc. – Speciale Banche dati*, 2009, p. 3 ss.); al riguardo v. anche FANUELE, Chiara, *Conservazione dei dati genetici e* privacy*: modelli stranieri e peculiarità italiane*, in *Dir. pen. e proc.*, 2011, p. 120.

[29] Alcuni Paesi (come Portogallo, Spagna, Belgio, Germania, Svizzera, Norvegia) hanno previsto l'immediata distruzione del campione a seguito delle analisi necessarie a ricavare il profilo genetico. In questo senso si è orientato anche il Regno Unito, a seguito dell'approvazione del *Protection of Freedom Act* del 2012; la regola generale prevede la distruzione del campione entro sei mesi dall'estrazione del profilo, ma sono contemplate eccezioni che permettono la conservazione per un periodo più lungo.

[30] FELICIONI, Paola, *Il regolamento di attuazione della Banca dati nazionale del dna: scienza e diritto si incontrano*, in *Dir. pen. proc.*, 2016, p. 712. Per alcuni

dei diritti individuali troppo elevato e non giustificato»[31]. Consapevole di dover fronteggiare questo genere di rilievi, il legislatore del 2009 ha affrontato con scrupolo la questione della "messa in sicurezza" dei dati custoditi (campioni e profili), apprestando presidi normativi, accorgimenti logicistici e cautele ad elevato coefficiente tecnologico.

L'*incipit* dell'art. 5 legge n. 85 del 2009 individua la finalità dell'istituzione della banca dati nazionale del dna nel «facilitare l'identificazione degli autori dei delitti», implicitamente escludendo che vi sia spazio tanto per l'acquisizione di dati eccedenti rispetto a questo scopo, quanto per ulteriori legittimi impieghi di profili e di campioni. L'indicazione teleologica trova conferma nell'art. 12 legge n. 85 del 2009, disposizione che ammette l'accesso ai dati conservati nella banca dati del dna e nel laboratorio centrale «esclusivamente per fini di identificazione personale»; quanto alle «finalità di collaborazione internazionale di polizia» evocate dalla medesima norma, non vanno intese come obiettivi diversi e aggiuntivi, ma, per coerenza, devono anch'esse limitarsi all'esclusivo scopo identificativo, sollecitato dalle autorità inquirenti di altri Stati. Significativamente, però, i presupposti per avviare la consultazione sono diversi a seconda che si tratti della banca dati in cui sono archiviati i profili del dna o del laboratorio centrale nel quale sono conservati i campioni biologici: nel primo caso, la polizia giudiziaria può sollecitarla autonomamente, nel secondo deve munirsi dell'autorizzazione dell'autorità giudiziaria[32]. In ogni caso, le richieste di consultazione provenienti dalle

esempi dell'utilità di conservare anche la conservazione del materiale cellulare v. LAGO, Giampietro, *Banche dati DNA: raccomandazioni internazionali, studio comparato con la Legge 85/2009*, cit., p. 150.

31 Così MONTI, Andrea, *Conservazione dei campioni biologici e tutela dei diritti fondamentali della persona*, in MARAFIOTI, Luca, LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Giuffrè, 2010, p. 55, sottolineando che «il campione biologico contiene tutta l'informazione: finché c'è una provetta in qualche laboratorio o deposito con una parte di mio materiale biologico, da quel campione è possibile fare una qualsiasi analisi, anche di tipo diagnostico» (p. 55, nota 1).

32 Sulla perimetrazione delle nozioni di polizia giudiziaria e autorità giudiziaria v. LAGO, Giampietro, *Il trattamento dei dati e dei campioni biologici: la banca dati nazionale del DNA e il bilanciamento tra le ragioni di giustizia e la tutela della* privacy, in SCARCELLA, Alessio (a cura di), *Prelievo del DNA e banca dati nazionale*, Cedam, 2009, p. 120 ss.

forze di polizia vanno motivate in relazione al procedimento penale in cui è emersa l'esigenza del raffronto[33].

Dall'impianto legislativo e dalla disciplina di attuazione, chiamata alla messa a punto dei dettagli tecnici, emergono due apprezzabili direttive. Rispetto agli accessi e alla natura delle operazioni compiute va assicurata la massima trasparenza, mediante l'identificazione di chiunque faccia ingresso fisicamente nei luoghi di conservazione e telematicamente nel *database*[34], come pure attraverso la registrazione di ogni attività – ingresso, consultazione, aggiornamento – che l'operatore ha compiuto e la conservazione delle relative registrazioni. Rispetto ai campioni biologici, ai profili del dna e alle generalità anagrafiche dei soggetti ai quali essi appartengono va garantita, al contrario, la massima inaccessibilità. Obiettivo al quale è rivolto più di un accorgimento. Anzitutto, profili e campioni sono conservati e gestiti in strutture distinte sul piano logistico e funzionale[35]: soluzione impegnativa, perché richiede al legislatore di regolamentare e controllare scrupolosamente il flusso di dati dall'una

---

[33] Una delicata valutazione alla quale è chiamato un ordinamento che si doti di una banca dati del dna attiene alle prerogative da riconoscere al difensore. Il dato normativo dell'art. 12 legge n. 85 del 2009 omette al riguardo qualsiasi riferimento rispetto alle *chance* del medesimo di interrogare l'archivio. Parte della dottrina ritiene che tale silenzio possa essere superato riconoscendo al difensore «il potere di chiedere al pubblico ministero l'autorizzazione all'esame presso la Banca dati e, se la pubblica accusa rigetta la richiesta, il difensore può proporre ricorso al giudice, al quale spetta di decidere» (TONINI, Paolo, *Informazioni genetiche e processo penale ad un anno dalla legge*, in *Dir. pen. proc.*, 2010, p. 886). Giudica tale lettura difficilmente praticabile CAMON, Alberto, *La disciplina delle indagini genetiche*, cit., p. 1445: dai lavori preparatori emerge che «non c'è una lacuna, suscettibile di essere colmata con l'analogia», e che «il difensore non è stato dimenticato, bensì volutamente estromesso».

[34] Nel Parere adottato il 28 luglio 2016 il Garante per la protezione dei dati personali aveva espresso l'esigenza che fossero apprestate misure di sicurezza a protezione delle aree di pertinenza della banca dati e del laboratorio centrale, sollecitando, tra l'altro, «ulteriori specificazioni (...) con riguardo a quali informazioni relative agli accessi fisici alle predette aree» sarebbero state registrate, «nonché ai tempi e alle modalità di conservazione».

[35] Una scelta analoga è stata compiuta dall'ordinamento francese, che distingue la banca dati, in cui si conservano i profili genetici, dal *Service Central de Préservation des Prélèvements Biologiques*, dove viene conservato il materiale biologico.

all'altra struttura[36], ma necessaria ad impedire quell'incrocio di dati che permetterebbe di ricavare «una quantità incontrollata di informazioni relative a un determinato soggetto», comportando un «rischio elevato di violazione della *privacy*»[37]. Conservare i profili genetici e operarne il raffronto compete alla banca dati nazionale del dna istituita presso il Dipartimento della pubblica sicurezza del Ministero degli interni: a dispetto della sua denominazione, si tratta di un *database* informatico puro, che «contiene soltanto informazioni digitalizzate»[38]. Tipizzare i profili genetici dai campioni biologici e provvedere alla conservazione di questi ultimi spetta, invece, al laboratorio centrale collocato presso il Ministero della giustizia, che è la vera biobanca. Entrambe queste strutture sono sottoposte a forme di sorveglianza: il controllo sulla banca dati è, comprensibilmente, affidato al Garante per la protezione dei dati personali; alla supervisione operativa sul laboratorio deve provvedere il Comitato nazionale per la biosicurezza, le biotecnologie e le scienze della vita, mentre al Garante, suscitando qualche perplessità in dottrina[39], è assegnato esclusivamente un compito consultivo rispetto alle verifiche che il Comitato deve eseguire presso il laboratorio.

Ambedue gli archivi, inoltre, contengono dati anonimizzati: per espressa prescrizione normativa, profili e campioni non devono essere contraddistinti da informazioni che consentano «l'identificazione diretta del soggetto cui sono riferiti» (art. 12 legge n. 85 del 2009)[40].

---

[36] Sul punto v. CALIFANO, Licia, *Il trattamento dei dati genetici: finalità di ricerca, esigenze di sicurezza e diritto alla protezione dei dati personali*, in *Cultura giuridica e diritto vivente*, 2017, n. 4, p. 7.

[37] COLOMBO, Eleonora, *Il nuovo regolamento per l'istituzione della banca dati nazionale del dna: commento a prima lettura e confronto con le disposizioni di altri Stati UE*, in *Cass. pen.*, 2016, p. 4617.

[38] MONTI, Andrea, *Ambiguità semantiche, finalità dei trattamenti e limiti operativi della* genetic evidence, in MARAFIOTI, Luca, LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Giuffrè, 2010, p. 34.

[39] COLAIACOVO, Cinzia, *Competenza del Garante per la protezione dei dati personali sull'applicazione del Trattato di Prüm*, in SCARCELLA, Alessio (a cura di), *Prelievo del DNA e banca dati nazionale*, Cedam, 2009, p. 189.

[40] La protezione delle informazioni è rafforzata dall'obbligo del segreto sugli atti, i dati, le informazioni di cui il personale addetto alla banca dati e al laboratorio sia venuto a conoscenza a causa dell'esercizio delle funzioni e presidiata penalmente dalla fattispecie incriminatrice che punisce il pubblico

Ogni soggetto "censito" è contraddistinto da una coppia di valori: «un numero identificativo univoco» viene generato al momento del prelievo dal sistema AFIS – che acquisisce e gestisce le impronte digitali – ed è «associato al suo profilo del dna»[41]. Soltanto nel caso in cui si registri una corrispondenza tra il profilo "anonimo" e uno di quelli conservati nella banca dati del dna sarà consentito risalire all'identità anagrafica del soggetto al quale appartiene, dato da comunicare agli organi inquirenti che hanno richiesto l'esplorazione. Decodificare il c.d. codice prelievo – ossia la stringa identificativa assegnata dal sistema AFIS al momento in cui il relativo campione è stato prelevato – non compete, tuttavia, agli operatori che si occupano di implementare e di gestire la banca dati; per evitare una concentrazione di competenze, pericolosa per la riservatezza, il decisivo passaggio finale è affidato al personale in servizio presso l'AFIS, al quale, per contro, ancora nell'ottica apprezzabile di evitare pericolosi incroci, è vietato accedere direttamente ai sistemi informativi della banca dati del dna e del laboratorio centrale[42].

---

ufficiale che, anche colposamente, comunica o fa uso di quei dati e di quelle informazioni «in violazione delle disposizioni del capo II della legge n. 85 del 2009 o al di fuori di fini previsti» dal medesimo.

41 Spiega BIONDO, Renato, *La Banca dati nazionale dna italiana*, in *Riv. it. med. leg.*, 2016, p. 217.

42 Lo sforzo legislativo per assicurare, ricorrendo a risorse tecnologicamente avanzate, la "messa in sicurezza" delle informazioni genetiche custodite nel laboratorio centrale e nella banca dati nazionale del dna mette in risalto l'inadeguatezza della disciplina del codice di rito penale quando il prelievo di materiale biologico avvenga nel corso del procedimento penale, ai fini di una perizia o di una consulenza tecnica (artt. 224-*bis* e 359-*bis* c.p.p.). Rispetto ai campioni biologici, emergono dal dato codicistico "spazi" per la conservazione, fino alla «definizione del procedimento con decreto di archiviazione» o alla pronuncia di una «sentenza non più soggetta ad impugnazione», provvedimenti ai quali consegue l'obbligo di procedere alla distruzione degli stessi. Quanto alla conservazione, tuttavia, mancano nell'art. 72-*quater* disp. att. c.p.p. indicazioni logistiche: taluno ritiene che competa alla cancelleria individuare un luogo adeguato, altri identificano tale luogo nel laboratorio in cui è avvenuta la tipizzazione dei profili, altri ancora affidano la conservazione del campione al perito; in mancanza di presidi normativamente imposti, nessuno degli scenari prefigurabili in via interpretativa appare tranquillizzante sul piano della riservatezza. Altrettanto sorprendentemente, il legislatore del 2009 si è disinteressato della sorte dei relativi profili. Un riferimento ai profili genetici ricavati dai campioni biologici prelevati nel corso del procedimento penale compare oggi nel d.P.R. n. 87 del 2016, il cui art. 35 prevede che

4. Il perimetro soggettivo del *database*

Nel dettare le coordinate dell'"anagrafe genetica", un legislatore che, avvalendosi delle più sofisticate strumentazioni tecnologiche, sia in grado di "blindare" i dati acquisiti potrebbe essere orientato a privilegiare soluzioni che ne massimizzino l'efficienza informativa a scopi di giustizia penale[43]. Si potrebbe ritenere, in altri termini, che *standard* più elevati di sicurezza autorizzino una maggiore estensione del patrimonio informativo custodito nel *database*, sul presupposto che, una volta efficacemente neutralizzati i rischi di indebiti "trattamenti" dei dati, non sarebbero prefigurabili ulteriori controindicazioni "da conservazione"[44].

---

vengano inseriti nella banca dati del dna anche i profili ricavati da «campioni biologici di soggetti che al momento del prelievo rientravano nelle previsioni dell'articolo 9 della legge acquisiti nel corso di procedimenti penali anteriormente alla data di entrata in funzione della banca dati». Se si intendeva sopperire alla predetta lacuna legislativa, si è proceduto in modo piuttosto maldestro. Non solo perché ad estendere ai profili ricavati dai campioni biologici l'immissione nella banca dati del dna che l'art. 10 legge n. 85 del 2009 limitava ai profili estratti dai reperti biologici è un regolamento di attuazione, dunque una fonte normativa di rango subordinato, ma anche perché quest'ultimo si occupa dei soli profili acquisiti nel procedimento penale dai campioni prelevati alle categorie individuate dall'art. 9 legge n. 85 del 2009. Per tutti gli altri soggetti che abbiano subìto il prelievo a fini investigativi o probatori la collocazione del relativo profilo continua dunque a risultare imprecisata. La sede più plausibile, secondo la dottrina, è rappresentata dal fascicolo processuale in cui il profilo è inserito (TONINI, Paolo, *Manuale di procedura penale*, Giuffrè, 2018, p. 600), ma dal punto di vista della "messa in sicurezza" dei dati in questione la soluzione non può che apparire insoddisfacente.

43 In questa direzione si era orientato in passato il Regno Unito, realizzando una «archiviazione dei dati genetici di tipo cosiddetto "pangenetico" o universale, tale da prevedere l'inserimento del maggior numero di dati acquisibili» (SCAFFARDI, Lucia, *Giustizia genetica e tutela della persona*, cit., p. 84).

44 «*A properly constructed universal DNA database would pose only a minimal invasion of privacy. In return, it would decrease crime, reverse and prevent false conviction, make investigations more effective and efficient, and protect against far more invasive investigative techniques. A universal DNA database should be viewed as a way to protect ourselves and others, not as a "Big Brother" invasion of privacy*», ritiene DEDRICKSON, Kristen, *Universal DNA databases: a way to improve privacy?*, in *Journal of Law and the Biosciences*, 2017, p. 647. Sui vantaggi di un «*universal genetic forensic database*» cfr. HAZEL, James, CLAYTON, Ellen, MALIN, Bradley, SLOBOGIN, Christopher, *Is it time for a universal genetic forensic database?*, in *Science*, 23 novembre 2018, p. 898 ss.

Per gli Stati aderenti alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali percorrere questa strada significherebbe esporsi alle probabili censure della Corte di Strasburgo[45]. Stando alla sua consolidata elaborazione, infatti, la conservazione dei dati genetici da parte di un'autorità pubblica integra un'ingerenza nel diritto al rispetto della vita privata e familiare[46] tutelato dall'art. 8 C.e.d.u., diritto nella cui poliedrica nozione i giudici europei ricomprendono anche gli aspetti legati all'identificazione personale e all'appartenenza, ricostruibile per via genetica, a un gruppo familiare[47].

Tale ingerenza appare tollerabile solo a condizione di soddisfare i requisiti previsti dall'art. 8 § 2 C.e.d.u.: oltre ad essere «prevista dalla legge», l'intromissione deve risultare «in una società democratica (...) necessaria» per il raggiungimento degli scopi individuati dalla norma in questione, tra cui figurano la sicurezza nazionale, la pubblica sicurezza, la difesa dell'ordine e la prevenzione dei reati. Anche là dove si riuscisse a garantire un livello molto elevato di protezione alle informazioni raccolte nella banca dati, dunque, nella prospettiva della Corte europea dei diritti dell'uomo la tutela della vita privata e familiare risulterebbe «indebolita in modo inaccettabile» in assenza di un «attento bilanciamento tra i vantaggi che possono derivare» alla giustizia penale dalla disponibilità dei dati genetici dei consociati e la tutela dei «fondamentali interessi che sono collegati al rispetto della vita privata»[48].

---

[45] Scarsamente propensa ad affidare «alla completa discrezionalità dei singoli Paesi i criteri di ingresso e di uscita dalla banca dati genetica», osserva SELLAROLI, Valentina, *Il "caso S. e Marper" e la Corte europea: il DNA e il bilanciamento tra opposte esigenze in una società democratica*, in *Leg. pen.*, 2009, p. 646.

[46] Più in generale, per la Corte di Strasburgo la conservazione di qualsiasi dato relativo alla vita privata di un soggetto costituisce di per sé un'ingerenza ai sensi dell'art. 8 C.e.d.u.: per tutti v. Corte eur. dir. uomo, 26 marzo 1987, Leander c. Svezia, § 48. Ciò indipendentemente dal fatto che tali dati siano effettivamente utilizzati, in quanto l'ingerenza nella vita privata si concretizza al momento della memorizzazione: così Corte eur. dir. uomo, 16 febbraio 2000, Amann c. Svizzera, § 69.

[47] Sulla capacità dimostrata dalla Corte di Strasburgo di utilizzare l'art. 8 C.e.d.u. come «baluardo contro forme di intrusione legate all'uso di tecnologie» avanzate, e, più in generale, di «estrapolare dalle scarne previsioni della Convenzione un sistema di regole e principi all'avanguardia» v. ALLEGREZZA, Silvia, *Prova scientifica e dimensione europea*, cit., p. 127.

[48] Corte eur. dir. uomo, 4 dicembre 2008, S. e Marper c. Regno Unito, § 112.

Per quanto il dettato della Convenzione europea dei diritti dell'uomo lasci al legislatore nazionale margini non trascurabili di apprezzamento, il concetto di "necessità" richiamato dall'art. 8 § 2 C.e.d.u. esclude la legittimità in chiave convenzionale di un'indiscriminata schedatura "di massa" dei consociati[49]. Omettendo ogni sforzo di assicurare un accettabile contemperamento degli interessi in conflitto, difficilmente supererebbe lo scrutinio dei giudici di Strasburgo la pretesa legislativa di includere nell'archivio genetico anche i profili di soggetti rispetto ai quali non possa formularsi alcuna prognosi sufficientemente plausibile di pericolosità sociale[50]. A ben poco varrebbe l'argomento secondo cui tanto più è consistente la quantità di informazioni genetiche a disposizione degli inquirenti, tanto più risultano elevate le probabilità di ricostruire la paternità delle tracce biologiche rilasciate nelle azioni criminose e, quindi, rafforzate le *chance* di prevenzione e di repressione dei reati. Al canone di "necessità" imposto dall'art. 8 C.e.d.u. è connaturata l'esigenza di una selezione dei soggetti da iscrivere nell'"anagrafe genetica", che il legislatore deve impegnarsi a soddisfare secondo parametri di ragionevolezza e di proporzionalità[51].

Nell'ordinamento italiano il delicato compito di tracciare lo spartiacque è affidato all'art. 9 legge n. 85 del 2009, che assoggetta a prelievo di campione – da cui estrarre il profilo destinato ad alimentare

---

[49] Di «un'archiviazione generalizzata dei profili genetici di tutta la popolazione, indipendentemente dal coinvolgimento in un procedimento penale», analizzano vantaggi, problematiche implicazioni e ostacoli normativi DAL MIGLIO, Chiara, GENTILOMO, Andrea, PICCININI Andrea, D'AURIA, Luca, *Dal prelievo coattivo alla banca dati dei profili genetici: l'ennesima incompiuta*, cit., p. 85. Individuano come prima contropartita di una banca dati a vocazione universale «*the high economic cost involved*» GUILLÉN, Margarina, LAREU, Marìa Victoria, PESTONI Carmela, SALAS, Antonio, CARRACEDO, Angel, *Ethical-legal problems of DNA databases in criminal investigation*, in *Journal of Medical Etichs*, 2000, f. 26, p. 267.

[50] Difficile da giustificare anche la necessità di sottoporli al prelievo del campione biologico da cui estrarre il profilo, eventualmente vincendone la resistenza con la forza.

[51] Un'esigenza analoga emergeva dalla Risoluzione del Consiglio del 9 giugno 1997 sullo scambio di risultati di analisi del DNA, là dove si affidava agli Stati membri dell'U.E. il compito di «stabilire a quali condizioni e per quali reati i risultati di analisi del DNA» possano «essere memorizzati in una banca dati nazionale».

la banca dati del dna – un'ampia gamma di soggetti: detenuti, condannati ammessi a una misura alternativa alla detenzione a seguito di sentenza irrevocabile, soggetti arrestati in flagranza di reato o sottoposti a fermo, destinatari di una misura custodiale (custodia cautelare in carcere, arresti domiciliari) e di una misura di sicurezza detentiva applicata in via provvisoria o definitiva. L'occasione "normativa" del prelievo funzionale ad alimentare il *database* è rappresentata, pertanto, da «un pregresso incidente giudiziario»[52], dal quale sia derivata una limitazione della libertà personale.

Non tutte le ipotesi di restrizione dello *status libertatis* alle quali il legislatore ha associato l'asportazione del campione presuppongono, oltre alla accertata o presunta responsabilità per un reato, anche una specifica valutazione della propensione dell'interessato a commettere illeciti penali[53]. In generale, la legge n. 85 del 2009 pare ritenere condizione sufficiente all'ingresso del profilo di un certo soggetto nella banca dati del dna che la responsabilità penale del medesimo sia stata accertata definitivamente oppure ipotizzata sulla base di elementi (i gravi indizi di colpevolezza, lo stato di flagranza) abbastanza solidi da aver superato il vaglio di un organo giurisdizionale (il giudice che ha applicato la custodia cautelare in carcere o gli arresti domiciliari, quello che ha convalidato l'arresto o il fermo). A ben vedere, nella prospettiva del legislatore – meno pacificamente secondo la dottrina – tanto l'accertamento definitivo della responsabilità penale[54] quanto la prefigurabilità di quest'ultima

---

[52] LEO, Guglielmo, *Il prelievo coattivo di materiale biologico nel processo penale e l'istituzione della Banca dati nazionale del DNA*, in *Riv. it. med. leg.*, 2011, p. 972.

[53] Tale valutazione ricorre, ad esempio, rispetto alle misure di sicurezza detentive applicate in via provvisoria o definitiva, alla custodia cautelare in carcere e agli arresti domiciliari disposti ai sensi dell'art. 274 comma 1 lett. *c*) c.p.p., all'arresto in flagranza giustificato dalla «pericolosità del soggetto desunta dalla sua personalità o dalle circostanze del fatto» *ex* art. 381 comma 4 c.p.p., idoneo a legittimare il prelievo purché sia stato convalidato.

[54] Affermano che «la prognosi di coinvolgimento in futuri procedimenti finisce per ridimensionare anche la presunzione di innocenza» ORLANDI, Renzo, PAPPALARDO, Giuseppe, *L'indagine genetica nel processo penale germanico. Osservazioni su una recente riforma*, cit., p. 768, in quanto «una persona è resa osservabile, grazie all'impronta genetica, per il suo modo d'essere, desunto essenzialmente dalla sua storia giudiziaria; vale a dire in ragione di una

sulla base di robusti indizi[55] integrano un «elemento prognostico (...) circa la futura commissione di reati»[56] in grado di giustificare sul piano funzionale l'acquisizione del profilo del soggetto in questione nel *database* rappresentativo dell'«attuale e/o probabile comunità criminale»[57].

A delimitare l'estensione dell'archivio provvede l'art. 9 comma 2 legge n. 85 del 2009: l'operazione di prelievo è consentita soltanto se il reato per cui si procede o si è proceduto rientra nel novero dei delitti non colposi per i quali è consentito l'arresto (almeno) facoltativo in flagranza. Letta in collegamento con la prognosi di pericolosità implicita nell'affermazione, definitiva o provvisoria, della colpevolezza, la scelta legislativa di circoscrivere il "censimento genetico" ai soggetti riconosciuti definitivamente responsabili o fortemente indiziati della commissione di un reato di gravità medio-alta pare esprimere una possibile traduzione

---

pericolosità presunta che lascia già intuire il coinvolgimento della persona stessa in prossime attività criminose».

55 Non condivide che la presunzione di pericolosità sociale formulata per i condannati venga estesa a chi è sottoposto a restrizione della libertà personale a titolo cautelare GALLUCCIO MEZIO, Gaetano, *Il prelievo di materiale biologico dalla persona sottoposta a restrizione della libertà personale in una recente pronuncia della Corte Suprema degli Stati Uniti*, in *Cass. pen.*, 2014, p. 1895, in quanto, «implicando l'equiparazione della persona gravemente indiziata di un'ipotesi di reato al colpevole, pare inconciliabile con la presunzione di innocenza riconosciuta all'imputato». *Contra*, GATTI, Emilio, *La Banca dati nazionale del Dna e la salvaguardia del diritto al rispetto della vita privata del singolo*, in *Quest. giust.*, 6 giugno 2018, secondo cui l'osservanza dell'art. 27 comma 2 Cost. è assicurata dalla cancellazione dei dati a seguito di assoluzione definitiva. Il Portogallo aveva inizialmente riservato l'ingresso in banca dati ai soli dati genetici dei soggetti condannati a una pena non inferiore a tre anni di reclusione. Con legge n. 90 del 2017, ha rivisto in senso estensivo la disciplina, ammettendo l'ingresso dei profili dei soggetti sospettati; in argomento v. SCAFFARDI, Lucia, *Giustizia genetica e tutela della persona*, cit., p. 149.

56 LEO, Guglielmo, *Il prelievo coattivo di materiale biologico nel processo penale e l'istituzione della Banca dati nazionale del DNA*, cit., p. 972.

57 L'espressione è di GENNARI, Giuseppe, *Bioinformazione e indagini penali: la l. n. 85 del 30 giugno 2009*, cit., p. 2634. Le categorie soggettive richiamate dall'art. 9 legge n. 85 del 2009 sono portatrici «per espressa presunzione normativa di una pericolosità qualificata – e *lato sensu* seriale – tale da giustificarne, anche per le caratteristiche criminologiche del reato espressivo, la profilazione e l'archiviazione del profilo genetico», ritiene ALVINO, Francesco, *La banca dati nazionale del DNA*, in ALVINO, Francesco, PRETTI, Davide, *Le indagini preliminari*, Giappichelli, 2017, p. 349.

del principio di proporzionalità insito nel riferimento alla necessità per esigenze preventive e di sicurezza contenuto nell'art. 8 § 2 C.e.d.u., come interpretato dalla Corte europea dei diritti dell'uomo[58]: il sacrificio che la conservazione del dato genetico in sé arreca alla *informational privacy* può dirsi legittimo solo nella prospettiva di prevenire la commissione o di consentire l'accertamento di fatti delittuosi che offendono beni giuridici di non trascurabile rilevanza[59].

Il legislatore italiano si dimostra cosciente, però, che una selezione dei profili da immettere nella banca dati del dna esclusivamente affidata al criterio della restrizione della libertà personale in riferimento a reati per cui è ammesso l'arresto in flagranza può non bastare ad impedire incursioni ingiustificate nella sfera della riservatezza genetica. Sono perciò sottratti al prelievo di campione biologico i soggetti accusati o condannati per una serie articolata di reati, il cui comune denominatore sembra essere la circostanza che alla condotta criminosa non si accompagna alcun rilascio di tracce biologiche. Al di là delle

---

[58] Nella sentenza Corte eur. dir. uomo, 4 dicembre 2008, S. e Marper c. Regno Unito, i giudici di Strasburgo si dicevano sorpresi dal carattere generale e indifferenziato con cui la legislazione inglese consentiva l'archiviazione dei dati genetici, sottolineando criticamente come la conservazione potesse essere disposta indipendentemente dalla natura e dalla gravità del reato di cui è sospettata la persona interessata nonché dall'età di quest'ultima. L'art. 9 legge n. 85 del 2009 valorizza in chiave selettiva natura e gravità del reato, ma non la minore età del soggetto passivo. La condizione anagrafica non è presa in considerazione neppure in riferimento a specifiche modalità operative di prelievo: il regolamento di attuazione si limita ad affermare che ad esso provvede, «sia per i soggetti minorenni che per gli adulti, il personale di Polizia penitenziaria, specificamente formato e addestrato», o, nei casi elencati dall'art. 5 comma 3, «il personale della forza di polizia delegata all'esecuzione del provvedimento restrittivo».

[59] Una soluzione di questo tipo era auspicata anche dal Garante per la protezione dei dati personali: «nel caso in cui il Parlamento ritenesse di prevedere che, in aggiunta ad una banca dati alimentata da informazioni raccolte per esigenze investigative nel corso dei procedimenti penali, alcune categorie di soggetti (quali fermati, arrestati, indagati, imputati o condannati per determinati reati) debbano essere sottoposti in ogni caso a un prelievo obbligatorio di cui va chiarita la specifica finalità, occorrerebbe comunque individuare in maniera selettiva e proporzionata i soggetti interessati e i relativi reati che non potrebbero che essere definiti sulla base della loro particolare gravità» (*Segnalazione al Parlamento e al Governo sulla disciplina delle banche dati del Dna a fini di giustizia*, 19 settembre 2007).

valutazioni che potrebbero formularsi circa l'esaustività dell'elencazione normativa, l'idea di fondo è che, se l'archiviazione del dato genetico in banca dati deve servire a far emergere eventuali recidive, conservare i profili dei soggetti accusati o condannati per determinati reati (ad esempio, reati tributari, fallimentari, in materia di intermediazione finanziaria, societari, contro la fede pubblica) non apporterebbe vantaggi in chiave preventiva o probatoria e, dunque, costituirebbe ingerenza non necessaria nella prospettiva dell'art. 8 C.e.d.u.[60].

5. Le cautele da adottare nella fase di prelievo

Un legislatore consapevole non può limitarsi a disciplinare nell'*an* il prelievo di materiale biologico; regolamentarne il *quomodo* è essenziale al duplice fine di garantire l'attendibilità delle informazioni destinate alla banca dati e di impedire che l'asportazione del campione si traduca in una operazione lesiva dei diritti individuali.

In relazione al primo obiettivo, mentre nel 2009 l'attenzione legislativa si è concentrata sulla fase successiva al prelievo, limitandosi a raccomandare l'immediato invio del campione biologico al laboratorio centrale tenuto a provvedere alla tipizzazione del profilo, il successivo regolamento di attuazione ha circondato di cautele dettagliate e "tecnologicamente avanzate" anche l'asportazione della mucosa del cavo orale e la catena di custodia: si prescrive che l'interessato venga preliminarmente identificato mediante il sistema AFIS relativo alle impronte digitali, si impone al personale incaricato del prelievo l'adozione di dispositivi di protezione individuale, si definiscono modalità di

[60] Per una interessante presa di posizione contro gli automatismi che trascurano l'aspetto qualitativo v. il Parere della Commissione nazionale per la protezione dei dati nazionali portoghese, *Paracer* n. 18/2007, in SCAFFARDI, Lucia, *Giustizia genetica e tutela della persona*, cit., p. 141: l'obbligo di essere sottoposto a prelievo biologico «solo per il fatto di essere stato condannato a più di tre anni di reclusione, indipendentemente dalla rilevanza del DNA per la fattispecie criminosa posta in essere», integra «un automatismo cieco rispetto al principio di proporzionalità, basato sulla formazione di un profilo criminogeno della personalità dell'imputato».

conservazione e di trasmissione al laboratorio centrale in grado di garantire l'integrità e la tracciabilità del campione[61].

Dal secondo punto di vista, l'art. 9 comma 4 legge n. 85 del 2009 non appare felicemente formulato: a rigore, richiamando il «prelievo di mucosa del cavo orale», allude all'asportazione del tessuto epiteliale che riveste la superficie interna della bocca. Nondimeno, le indicazioni esecutive fornite dal regolamento attuativo supportano una lettura maggiormente in sintonia con il principio di minima offensività e con le raccomandazioni europee[62], che riferisce l'asportazione alle «particelle di desquamazione della mucosa orale che si possono trovare nella saliva»[63]: il prescritto impiego di un tampone orale a secco «strofinato sulla parte interna della guancia ovvero sulle gengive per un tempo adeguato» sembra, infatti, tecnica conforme all'esecuzione del meno invasivo prelievo salivare.

Poco attenta ad individuare la tipologia di asportazione meno offensiva, la disciplina del 2009 raccomanda all'organo procedente – che il dato normativo vuole «specificamente formato e addestrato» – di operare nel «rispetto della dignità, del decoro e della riservatezza» dell'interessato[64] e si sforza di dissuaderlo dal porre in essere comportamenti non ortodossi: oltre a imporgli di redigere un verbale delle operazioni effettuate, fa discendere dalla «violazione delle disposizioni previste dall'articolo 9» – espressione idonea a ricomprendere sia i casi di prelievo indebito, sia le ipotesi di asportazione gratuitamente offensiva – la distruzione del

---

61 Scopo, quest'ultimo, al quale risponde più in generale la procedura informatizzata riservata ai soli operatori autorizzati che assicura la gestione del flusso del campione biologico dalla fase dell'asportazione all'arrivo nella sede del laboratorio centrale (art. 5 comma 7 d.P.R. n. 87 del 2016).

62 L'esigenza di farsi carico delle possibili implicazioni del prelievo sulla sfera dei diritti individuali era affiorata già in sede europea: la Risoluzione del Consiglio del 9 giugno 1997 sullo scambio di risultati di analisi del DNA si preoccupava di assicurare che «la raccolta di materiale DNA ai fini della memorizzazione» fosse «corredata di garanzie per la protezione dell'integrità fisica» degli interessati. Sulla necessità che il prelievo di campioni biologici si realizzi con metodiche rispettose della dignità della persona e del suo diritto alla salute v. Corte eur. dir. uomo, 11 giugno 2006, Jalloh c. Germania, §§ 67 ss.

63 FELICIONI, Paola, *Il regolamento di attuazione della Banca dati nazionale del dna: scienza e diritto si incontrano*, cit., p. 731.

64 Cfr. l'art. 9 commi 4 e 5 legge n. 85 del 2009.

campione biologico e la cancellazione del profilo tipizzato, privando così le condotte *contra legem* di utilità investigativa[65].

Difetta, tuttavia, una specifica attenzione normativa nei confronti dell'eventualità in cui il soggetto opponga resistenza al prelievo; un aspetto che un legislatore accorto non dovrebbe lasciare alla gestione, non di rado disinvolta, della prassi, dal momento che l'asportazione forzosa di un campione biologico – come affermato dalla Corte costituzionale rispetto al prelievo ematico coattivo – «non solo interessa la sfera della libertà personale, ma la travalica perché, seppure in minima misura, invade la sfera corporale della persona»[66].

Interferendo con la libertà personale, nell'ordinamento italiano la disciplina dell'asportazione coattiva di materiale biologico deve collocarsi all'interno delle coordinate dell'art. 13 comma 2 Cost. Ebbene, mentre i casi e i modi dell'ablazione risultano sufficientemente definiti dall'art. 9 legge n. 85 del 2009, meno scontata è la capacità dell'attuale disciplina di soddisfare la necessità costituzionalmente imposta che il prelievo si fondi su un «atto motivato dell'autorità giudiziaria»[67].

Anche quando si rende necessario vincere con la forza la resistenza dell'interessato all'asportazione, la disciplina prescinde discutibilmente dall'autorizzazione *ad hoc* dell'organo giurisdizionale; garanzia non surrogabile da «provvedimenti amministrativi motivati», i quali, «tenuto conto delle circostanze di fatto, diano atto delle ragioni che hanno reso necessaria la coercizione al fine di vincere la resistenza passiva del detenuto al prelievo»[68]. Il prelievo *de quo* non pare in alcun

---

[65] Cfr., rispettivamente, gli artt. 9 comma 5 e 13 comma 3 legge n. 85 del 2009.

[66] Così Corte cost., 9 luglio 1996, n. 238, dichiarando l'illegittimità costituzionale dell'art. 224 comma 2 c.p.p. «nella parte in cui consente che il giudice, nell'ambito delle operazioni peritali, disponga misure che comunque incidano sulla libertà personale dell'indagato o dell'imputato o di terzi, al di fuori di quelle specificamente previste nei "casi" e nei "modi" dalla legge».

[67] Ritiene possa essere identificato nello «stesso atto impositivo della restrizione» della libertà personale, «tra i cui effetti *lato sensu* esecutivi si annovera ora, *ex lege*, l'identificazione genetica dell'interessato», ALVINO, Francesco, *La banca dati nazionale del DNA*, cit., p. 349, nota 19.

[68] Cfr. invece la circolare D.a.p. del 26 ottobre 2016, avente a oggetto «Laboratorio centrale per la banca dati del DNA. Problematica inerente il prelievo coattivo del campione biologico del DNA in caso di rifiuto del ristretto».

modo riconducibile alle «misure di trattamento rientranti nell'ambito di competenza» dell'amministrazione penitenziaria, eccezionalmente sottratte, secondo la giurisprudenza costituzionale[69], all'osservanza delle garanzie di cui all'art. 13 Cost. perché «attinenti alle modalità concrete (...) di attuazione del regime carcerario in quanto tale, e dunque già potenzialmente ricomprese nel *quantum* di privazione della libertà personale conseguente allo stato di detenzione»; a ben vedere, il prelievo coattivo di campioni biologici comporta una limitazione della libertà personale aggiuntiva rispetto allo *status detentionis* e non funzionale a soddisfare «ragioni di ordine o di sicurezza» essenziali al suo mantenimento.

6. I tempi di conservazione: le scelte normative

Nell'assetto delineato dalla legge n. 85 del 2009, a determinare la soppressione dei campioni biologici conservati nel laboratorio centrale e la cancellazione dei profili archiviati nella banca dati nazionale del dna sono ragioni processuali o, in alternativa, fattori temporali. Nel primo caso, i predetti esiti conseguono all'irrevocabilità di una sentenza di assoluzione adottata perché il fatto non sussiste, l'imputato non lo ha commesso, il fatto non costituisce reato o il fatto non è previsto dalla legge come reato[70].

---

[69] Corte cost., 22 novembre 2000, n. 526.

[70] Considerata l'attenzione peculiare riservata dalla Corte di Strasburgo all'esigenza che i minori nei cui confronti non sia stata emessa una sentenza di condanna «siano protetti da qualsiasi pregiudizio», in riferimento al «loro sviluppo e (alla) loro integrazione nella società», derivante dal fatto che «le autorità pubbliche, successivamente alla assoluzione, decidano di conservarne i dati personali (Corte eur. dir. uomo, 4 dicembre 2008, S. e Marper c. Regno Unito, § 124), in dottrina si ritiene che l'elenco delle formule da cui far derivare la cancellazione immediata dei dati relativi agli infradiciottenni debba comprendere, «per ridurre al minimo il pericolo di stigmatizzazione», anche «le sentenze di non luogo a procedere per irrilevanza del fatto, la concessione del perdono giudiziale, l'estinzione del reato per esito positivo della prova, la declaratoria di una causa di immaturità del minore, la declaratoria della non imputabilità per il minore di anni quattordici» (CAPITTA, Anna Maria, *Conservazione dei DNA* profiles *e tutela europea dei diritti dell'uomo*, in *Arch. pen.*, 2013, n. 1, p. 30).

Si tratta di una cancellazione «riabilitativa»[71], doverosamente associata dal legislatore alla definitiva smentita in sede giudiziale dell'ipotizzato collegamento tra il soggetto "schedato" e uno dei reati elencati dall'art. 9 legge n. 85 del 2009, che aveva rappresentato il presupposto della misura restrittiva della libertà personale a suo carico e del correlato prelievo del campione[72].

In assenza di un'assoluzione definitiva con formula ampiamente liberatoria, l'eliminazione dei dati genetici dalla banca dati del dna e dal laboratorio centrale consegue al decorso di un periodo differentemente individuato a seconda della tipologia del dato. Il legislatore del 2009 si era limitato a individuare i termini massimi di conservazione ai quali il regolamento di attuazione avrebbe dovuto attenersi: per il campione biologico, venti anni dall'ultimo prelievo; per il profilo del dna, quaranta anni dall'ultima circostanza che ne ha determinato l'inserimento[73].

Il d. lgs. n. 87 del 2016 pare aver tenuto conto delle perplessità dottrinarie circa la compatibilità di tali proiezioni temporali con il principio di proporzionalità[74]. Rispetto ai soggetti "schedati" nei cui confronti non è

---

[71] La definizione è di FELICIONI, Paola, *La prova del DNA nel procedimento penale*, Giuffrè, 2018, p. 378.

[72] La circostanza che la legislazione francese non prevedesse nel caso di assoluzione di un soggetto la cancellazione delle sue impronte digitali dallo schedario automatizzato in cui erano conservate è stata censurata per violazione dell'art. 8 C.e.d.u. da Corte eur. dir. uomo, 18 aprile 2013, M.K. c. Francia, in *Dir. pen. proc*., 2013, p. 809 ss. Per i possibili riflessi della decisione nel nostro ordinamento v. SCARCELLA, Alessio, *Conservazione delle impronte digitali degli "assolti" e violazione dell'art. 8 Conv. e.d.u*., in *Dir. pen. proc*., 2013, p. 823 ss.

[73] In riferimento al *range* temporale individuato dalla legge n. 85 del 2009 v. D'AMATO, Antonio, *La banca-dati nazionale del Dna e le modifiche al codice di procedura penale in tema di prelievi coattivi di materiale biologico a fini di prova*, in *Critica pen*., 2009, p. 223: «il funzionamento della banca-dati nazionale è legata al fenomeno della recidiva: le possibilità che il profilo del DNA di un soggetto arrestato per un qualsivoglia reato sia riconosciuto corrispondente alle tracce di un altro reato aumentano in proporzione all'ampiezza del lasso temporale in cui tale confronto è possibile; al di sotto di un limite minimo l'archivio potrebbe risultare inutile (tenendo conto di un primo periodo in cui il soggetto resta detenuto)».

[74] Per tutti, cfr. SANTOSUOSSO, Amedeo, COLUSSI, Ilaria Anna, *La banca dati del DNA: questioni in tema di alimentazione, trattamento e accesso, presupposti, cancellazione e tempi di conservazione (artt. 5-15 l. n. 85/09)*, cit., p. 459;

intervenuta un'assoluzione definitiva nel merito, il regolamento ha fissato il periodo di conservazione del campione nel laboratorio centrale in otto anni, che corrispondono alla sua fisiologica durata[75]; quanto al profilo genetico, ha introdotto un doppio binario temporale: la permanenza ordinaria all'interno della banca dati si protrae per trenta anni a partire dall'ultima registrazione[76]; diventa di quaranta anni quando il profilo archiviato appartiene a un soggetto dichiarato recidivo con sentenza definitiva – condizione che rafforza la prognosi di "pericolosità sociale" a suo carico, su cui si fonda di per sé l'acquisizione in banca dati del suo profilo genetico – o condannato con sentenza irrevocabile per reati di particolare gravità e natura[77], in sintonia con i suggerimenti formulati dai giudici di Strasburgo[78].

7. ... e gli aspetti da rimeditare

A ben vedere, l'orizzonte trentennale di conservazione nella banca dati nazionale del dna riguarda i profili non soltanto dei condannati in via definitiva ma anche di coloro che, dopo essere stati ristretti nella libertà perché sospettati della commissione di un reato, siano destinatari di un

FANUELE, Chiara, *Conservazione dei dati genetici e* privacy*: modelli stranieri e peculiarità italiane*, cit., p. 129.

75 Più precisamente, ai sensi dell'art. 24 d.P.R. n. 87 del 2016, «il Dna estratto dai campioni biologici, dopo la sua completa tipizzazione deve essere distrutto» (comma 1), mentre «la parte del campione biologico non utilizzata ed il secondo campione di riserva sono conservati per un periodo di otto anni» (comma 3).

76 Condivide la scelta legislativa di abbreviare, rispetto alla soglia massima consentita dalla legge n. 85 del 2009, i termini di conservazione dei profili genetici FANUELE, Chiara, *Il regolamento attuativo della banca dati nazionale del DNA: nuove garanzie e preesistenti vuoti di tutela*, in *Proc. pen. giust*., 2017, p. 129, ritenendola espressione di «un bilanciamento più efficace tra il diritto alla *privacy* e le esigenze di protezione della collettività».

77 Si tratta dei reati per i quali è previsto l'arresto obbligatorio in flagranza e dei reati ricompresi nel nutrito elenco dell'art. 407 comma 2 lett. *a*) c.p.p., in cui figurano, tra gli altri, il reato di associazione di tipo mafioso, il reato di tratta di persone, reati con finalità di terrorismo o di eversione costituzionale, reati in materia sessuale.

78 In questo senso v. Corte eur. dir. uomo, 22 giugno 2017, Aycaguer c. Francia, in *Dir. proc. pen*., 2017, p. 1389.

provvedimento di archiviazione per infondatezza della *notitia criminis* o di una sentenza di non luogo a procedere con le formule il fatto non sussiste, l'imputato non lo ha commesso, il fatto non è previsto dalla legge come reato, il fatto non costituisce reato[79].

Probabilmente sulla scelta di non associare a tali epiloghi del procedimento la distruzione del campione e l'eliminazione del profilo hanno inciso pragmatiche valutazioni "di economia": qualora sopravvenissero elementi in grado di determinare la riapertura delle indagini o la revoca della sentenza di non luogo a procedere, il procedimento penale riprenderebbe il suo corso e potrebbe concludersi con una sentenza di condanna a pena detentiva, che imporrebbe di effettuare nuovamente il prelievo del campione biologico e la tipizzazione del relativo profilo genetico, ove gli stessi fossero stati già soppressi[80].

Pare tuttavia eccessivo che l'ordinamento si faccia carico a tal punto di tali esigenze, legate all'ipotetico verificarsi di circostanze neppure così frequenti, da omologare, sul piano della permanenza dei profili nella banca dati del dna, le due categorie soggettive appena richiamate ai condannati con sentenza irrevocabile[81]: almeno quando un provvedimento giudiziale, ancorché non definitivo, abbia escluso i presupposti di merito per esercitare l'azione penale nei riguardi di un soggetto "schedato" o per trarlo a giudizio, il legislatore avrebbe dovuto, se non necessariamente

---

[79] Secondo GENNARI, Giuseppe, *Bioinformazione e indagini penali: la l. n. 85 del 30 giugno 2009*, cit., p. 2636, in tal modo il legislatore considera «perenni sospetti coloro che hanno visto archiviare la indagine a loro carico e coloro che vengono prosciolti in udienza preliminare», compiendo una scelta «palesemente incostituzionale» e altresì «paradossale», in quanto l'indagato «da subito ritenuto non meritevole di un processo per carenza di elementi di accusa in grado di giustificare un dibattimento si trova ad avere un trattamento peggiore di chi riesce a dimostrare la propria innocenza solo dopo tre gradi di giudizio».

[80] In senso critico rispetto alla soluzione legislativa v. anche SCAFFARDI, Lucia, *Giustizia genetica e tutela della persona*, cit., p. 245, secondo cui «il criterio di definitività del procedimento (...) non appare ragionevole e proporzionato rispetto al fine che si intende perseguire».

[81] Introducendo così una difformità di trattamento – a parità di presupposti "proscioglitivi" – rispetto agli assolti in via definitiva che la differenza sul piano della "stabilità" del provvedimento tra archiviazione e sentenza di non luogo a procedere, da un lato, e assoluzione irrevocabile, dall'altro, potrebbe non essere sufficiente a giustificare.

prevedere la soppressione immediata dei relativi profilo e campione, almeno stabilire una ingerenza "da conservazione" più circoscritta nel tempo[82] rispetto a quella imposta a chi abbia visto accertata in via definitiva la propria responsabilità penale[83].

L'opportunità di differenziare l'orizzonte temporale di conservazione pare trovare riscontro anche nella giurisprudenza della Corte europea dei diritti dell'uomo, che nel 2008 ha definito «particolarmente preoccupante (...) il rischio di stigmatizzazione che discende» dall'equiparazione, allora operata dalla legislazione inglese sul piano dei tempi di permanenza dei dati genetici nella banca dati del dna, tra i *criminal suspects* (soggetti «che non sono stati riconosciuti colpevoli di nessun reato») e i condannati[84]. È vero che in quel caso il comune trattamento prevedeva la conservazione a tempo indefinito dei dati immessi nel *database*, soluzione scartata dalla legge n. 85 del 2009. Tuttavia, anche considerando che il periodo di conservazione stabilito dal regolamento di attuazione risulta tutt'altro che trascurabile, tale accorgimento potrebbe non bastare a sottrarre la disciplina italiana alle censure dei giudici di Strasburgo, piuttosto attenti al rispetto dei canoni di ragionevolezza e proporzionalità quando si tratta di ingerenze legislative nella sfera privata e familiare.

BIBLIOGRAFIA

ALLEGREZZA, Silvia. *Prova scientifica e dimensione europea*, in CANZIO, Giovanni, LUPARIA, Luca (a cura di), *Prova scientifica e processo penale*, Milano: Giuffrè, 2018, p. 125 ss.

---

[82] Ad esempio, l'ordinamento scozzese, accanto alla regola generale che impone la distruzione di campioni e profili relativi a soggetti non condannati, ha introdotto la possibilità eccezionale di conservare il profilo genetico di soggetti accusati ma non condannati per «*specific relevant sexual or violent offences*» per un periodo di tre anni, eventualmente prorogabile per altri due.

[83] Soluzione preferibile secondo CAPITTA, Anna Maria, *Conservazione dei DNA* profiles *e tutela europea dei diritti dell'uomo*, cit., p. 29, a tutela del principio della presunzione di innocenza di cui all'art. 27 comma 2 Cost. e del diritto alla non stigmatizzazione, espressione del "giusto processo" di cui all'art. 111 comma 1 Cost.

[84] Corte eur. dir. uomo, 4 dicembre 2008, S. e Marper c. Regno Unito, § 122.

ALVINO, Francesco. *La banca dati nazionale del DNA*, in ALVINO, Francesco, PRETTI, Davide, *Le indagini preliminari*, Torino: Giappichelli, 2017, p. 349 ss.

BIONDO, Renato. *La Banca dati nazionale dna italiana*, in *Riv. it. med. leg.*, 2016, p. 213 ss.

CALIFANO, Licia. *Il trattamento dei dati genetici: finalità di ricerca, esigenze di sicurezza e diritto alla protezione dei dati personali*, in *Cultura giuridica e diritto vivente*, 2017, n. 4.

CAMON, Alberto. *La disciplina delle indagini genetiche*, in *Cass. pen.*, 2014, p. 1426 ss.

CAPITTA, Anna Maria. *Conservazione dei DNA* profiles *e tutela europea dei diritti dell'uomo*, in *Arch. pen.*, 2013, n. 1.

COCITO, Andrea. *Parametri internazionali e affidabilità dei laboratori nelle analisi dei reperti e campioni*, in MARAFIOTI, Luca, LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Milano: Giuffrè, 2010, p. 91 ss.

COLAIACOVO, Cinzia. *Competenza del Garante per la protezione dei dati personali sull'applicazione del Trattato di Prüm*, in SCARCELLA, Alessio (a cura di), *Prelievo del DNA e banca dati nazionale*, Padova: Cedam, 2009, p. 189 ss.

COLOMBO, Eleonora. *Il nuovo regolamento per l'istituzione della banca dati nazionale del dna: commento a prima lettura e confronto con le disposizioni di altri Stati UE*, in *Cass. pen.*, 2016, p. 4615 ss.

DAL MIGLIO, Chiara; GENTILOMO, Andrea; PICCININI Andrea; D'AURIA, Luca. *Dal prelievo coattivo alla banca dati dei profili genetici: l'ennesima incompiuta*, in *Riv. it. dir. med. leg.*, 2007, p. 61 ss.

DEDRICKSON, Kristen. *Universal DNA databases: a way to improve privacy?*, in *Journal of Law and the Biosciences*, 2017, p. 647 ss.

FANUELE, Chiara. *Conservazione dei dati genetici e* privacy*: modelli stranieri e peculiarità italiane*, in *Dir. pen. e proc.*, 2011, p. 129 ss.

FANUELE, Chiara. *Il regolamento attuativo della banca dati nazionale del DNA: nuove garanzie e preesistenti vuoti di tutela*, in *Proc. pen. giust.*, 2017, p. 129 ss.

FASSONE, Elvio. *Le scienze come ausilio nella ricerca del fatto e nel giudizio di valore*, in DE CATALDO NEUBURGER, Luisa (a cura di), *La prova scientifica nel processo penale*, Padova: Cedam, 2007, p. 247 ss.

FELICIONI, Paola. *DNA e Banche dati europee*, in AA. VV., *Investigazioni e prove transnazionali*, Milano: Giuffrè, 2017, p. 177 ss.

FELICIONI, Paola. *Il regolamento di attuazione della Banca dati nazionale del dna: scienza e diritto si incontrano*, in *Dir. pen. proc*., 2016, p. 712 ss.

FELICIONI, Paola. *La prova del DNA nel procedimento penale*, Milano: Giuffrè, 2018.

GALLUCCIO MEZIO, Gaetano. Il prelievo di materiale biologico dalla persona sottoposta a restrizione della libertà personale in una recente pronuncia della Corte Suprema degli Stati Uniti, in *Cass. pen*., 2014, p. 1895 ss.

GATTI, Emilio. La Banca dati nazionale del Dna e la salvaguardia del diritto al rispetto della vita privata del singolo, in *Quest. giust*., 6 giugno 2018.

GENNARI, Giuseppe. Bioinformazione e indagini penali: la l. n. 85 del 30 giugno 2009, in *Resp. civ. e prev*., 2009, p. 2630 ss.

GENNARI, Giuseppe. Genetica forense e codice della privacy: riflessioni su vecchie e nuove banche dati, in *Resp. civ. e prev*., 2011, p. 1184 ss.

GENNARI, Giuseppe. *La istituzione della banca dati del Dna ad uso forense: dalla* privacy *alla sicurezza*, in SCARCELLA, Alessio (a cura di), *Prelievo del DNA e banca dati nazionale*, Padova: Cedam, 2009, p. 71 ss.

GUILLÉN, Margarina. LAREU, Marìa Victoria, PESTONI Carmela, SALAS, Antonio, CARRACEDO, Angel, *Ethical-legal problems of DNA databases in criminal investigation*, in *Journal of Medical Etichs*, 2000, f. 26, p. 267 ss.

HAZEL, James; CLAYTON, Ellen; MALIN, Bradley; SLOBOGIN, Christopher. *Is it time for a universal genetic forensic database?*, in *Science*, 23 novembre 2018, p. 898 ss.

LAGO, Giampietro. *Banche dati DNA: raccomandazioni internazionali, studio comparato con la Legge 85/2009*, in *Giust. pen*., 2010, p. 142 ss.

LAGO, Giampietro. *Il trattamento dei dati e dei campioni biologici: la banca dati nazionale del DNA e il bilanciamento tra le ragioni di giustizia e la tutela della* privacy, in SCARCELLA, Alessio (a cura di), *Prelievo del DNA e banca dati nazionale*, Padova: Cedam, 2009, p. 120 ss.

LEO, Guglielmo. *Il prelievo coattivo di materiale biologico nel processo penale e l'istituzione della Banca dati nazionale del DNA*, in *Riv. it. med. leg*., 2011, p. 931 ss.

LUPARIA, Luca. *Dati genetici e cultura processuale: un futuro ancora da comporre*, in MARAFIOTI, Luca, LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Milano: Giuffrè, 2010, p. 348 ss.

MARAFIOTI, Luca. *Le banche dati del dna. Una nuova frontiera investigativa nel trattato di Prüm*, in MARAFIOTI, Luca-LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Milano: Giuffrè, 2010, p. 8 ss.

MONTI, Andrea. *Ambiguità semantiche, finalità dei trattamenti e limiti operativi della* genetic evidence, in MARAFIOTI, Luca, LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Milano: Giuffrè, 2010, p. 34 ss.

MONTI, Andrea. *Conservazione dei campioni biologici e tutela dei diritti fondamentali della persona*, in MARAFIOTI, Luca, LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Milano: Giuffrè, 2010, p. 55 ss.

ORLANDI, Renzo. *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, p. 1155 ss.

ORLANDI, Renzo; PAPPALARDO, Giuseppe. *L'indagine genetica nel processo penale germanico. Osservazioni su una recente riforma*, in *Dir. proc. pen.*, 1999, p. 767 ss.

PRESUTTI, Adonella. *L'acquisizione forzosa dei dati genetici tra adempimenti internazionali e impegni costituzionali*, in *Riv. it. dir. proc. e pen.*, 2010, p. 548 ss.

RICCI, Ugo; PREVIDERÈ, Carlo; FATTORINI, Paolo; CORRADI, Fabio. *La prova del dna per la ricerca della verità*, Milano: Giuffrè, 2006, p. 30 ss.

RICCI, Ugo. *Un lampo di consapevolezza nella normativa italiana: il DNA oltre la suggestione e il mito*, in *Dir. pen. proc.*, 2016, p. 743 ss.

RODOTÀ, Stefano. *Difendere i cittadini dagli abusi della scienza*, in *La Repubblica*, 6 gennaio 1999.

SALSI, Giancarlo. *La Banca Dati del DNA. Indagini genetiche e problematiche giuridiche*, Bologna: Clueb, 2012.

SANTOSUOSSO, Amedeo; COLUSSI, Ilaria Anna. *La banca dati del DNA: questioni in tema di alimentazione, trattamento e accesso, presupposti, cancellazione e tempi di conservazione (artt. 5-15 l. n. 85/09)*, in *Pol. dir.*, 2011, p. 457 ss.

SCAFFARDI, Lucia. *Giustizia genetica e tutela della persona*, Padova: Cedam, 2017.

SCARCELLA, Alessio. *Conservazione delle impronte digitali degli "assolti" e violazione dell'art. 8 Conv. e.d.u.*, in *Dir. pen. proc.*, 2013, p. 823 ss.

SCOLLO, Giancarlo. *La disciplina attuativa della banca dati del dna e del laboratorio centrale*, in MARAFIOTI, Luca, LUPARIA, Luca (a cura di), *Banca dati del DNA e accertamento penale*, Milano: Giuffrè, 2010, p. 165 ss.

SELLAROLI, Valentina. *Il "caso S. e Marper" e la Corte europea: il DNA e il bilanciamento tra opposte esigenze in una società democratica*, in *Leg. pen.*, 2009, p. 646 ss.

SIGNORATO, Silvia. *Il trattamento dei dati personali per fini di prevenzione e repressione penale*, in *Riv. dir. proc.*, 2015, p. 1492 ss.

TONINI, Paolo. *Accertamento del fatto e informazioni genetiche: un difficile bilanciamento*, in *Dir. pen. proc. – Speciale Banche dati*, 2009, p. 3 ss.

TONINI, Paolo. *Informazioni genetiche e processo penale ad un anno dalla legge*, in *Dir. pen. proc.*, 2010, p. 883 ss.

TONINI, Paolo. *Manuale di procedura penale*, Milano: Giuffrè, 2018.

Informações adicionais e declarações dos autores (*integridade científica*)

Declaração de conflito de interesses (conflict of interest declaration): a autora confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

Declaração de ineditismo e originalidade (declaration of originality): a autora assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 10/7/2019
- Controle preliminar e verificação de plágio: 23/7/2019
- Avaliação 1: 7/10/2019
- Avaliação 2: 8/10/2019
- Decisão editorial preliminar: 8/9/2019
- Retorno rodada de correções: 17/10/2019
- Decisão editorial final: 17/10/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editoras-associadas: 2 (CC e BC)
- Revisores: 2

COMO CITAR ESTE ARTIGO:

GABRIELLI, Chiara. L'archiviazione dei dati genetici a fini di giustizia penale: gli interessi in gioco, le prescrizioni europee, le soluzioni adottate dal legislatore italiano. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1385-1420, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.258

L'escalation dei mezzi di intrusione nella sfera privata: ripartire dalla Costituzione[1]

The escalation of the means of intrusion into the private sphere: starting from the Constitution

A ampliação dos meios de intrusão na esfera privada: repensar a partir da Constituição

Fabio Alonzi[2]

Università degli Studi di ROMA "La Sapienza" - Italia

fabio.alonzi@tiscali.it

http://orcid.org/0000-0002-3570-9939

Riassunto: Gli artt. 13, 14 e 15 della Costituzione italiana proclamano i "principi" dell'intangibilità della libertà personale, di domicilio e delle comunicazioni, prevedendo un'articolata disciplina che si fa carico di indicare le condizioni minime per tollerare atti invasivi di queste libertà. Il proliferare di nuove pericolose forme tecnologiche di invasività dematerializzate della sfera personale sembra mettere in crisi queste tutele costituzionali che solo una rivitalizzazione della categoria dell'inviolabilità dei diritti fondamentali della persona consente di rafforzare, fornendo allo stesso tempo le basi concettuali per l'introduzione e la valorizzazione di nuovi strumenti di garanzia quale quello di "domicilio informatico".

Parole-chiave: Processo penale italiano; indagini informatiche; diritti fondamentali.

[1] Il presente testo, riveduto ed ampliato, è lo sviluppo della relazione svolta al convegno del Centro studi giuridici e sociali "Aldo Marongiu" (Unione delle Camere Penali Italiane): *Nei limiti della Costituzione. Il codice repubblicano e il processo penale contemporaneo* (Roma, 28-29 settembre 2018).

[2] Dottore di ricerca in diritto e procedura penale, "Sapienza" Università di Roma.

Abstract: *Articles 13, 14 and 15 of the Italian Constitution proclaim the "principles" of the inviolability of personal freedom, of domicile and communications by providing an articulated discipline that takes care of indicating the minimum conditions to tolerate invasive acts of these freedoms. The proliferation of new dangerous technological forms of dematerialized invasiveness of the personal sphere seem to undermine these constitutional protections that only a revitalization of the category of inviolability of the fundamental rights of the person allows to strengthen, providing at the same time the conceptual bases for the introduction and enhancement of new guarantee instruments such as "IT domicile".*

Keywords: *Italian criminal procedure; IT investigation; fundamental rights.*

Resumo: *Os artigos 13, 14 e 15 da Constituição italiana proclamam os "princípios" da intangibilidade da liberdade pessoal, do domicílio e das comunicações prevendo uma articulada disciplina que regula as condições mínimas para que se autorizem medidas invasivas a essas liberdades. A proliferação de novas e perigosas formas tecnológicas de medidas invasivas imateriais na esfera pessoal parecem colocar em crise essas limitações constitucionais. Por outro lado, somente uma revitalização da categoria da inviolabilidade dos direitos fundamentais permitiria reforçar e, ao mesmo tempo, fornecer as bases conceituais para a introdução e a valorização de novos instrumentos de garantia como aquela de "domicílio informático".*

Palavras-chave: *Processo penal italiano; investigação informática; direitos fundamentais.*

1. Processo penale e Costituzione: un legame indissolubile

Il titolo che gli organizzatori hanno dato all'odierno convegno ci invita a riflettere su quale sia l'effettiva forza connotativa dei principi della nostra Costituzione sulla disciplina del processo penale.

L'occasione è offerta da un duplice anniversario: l'entrata in vigore della nostra Carta fondamentale e l'approvazione dell'attuale codice di rito.

Come avviene per le vite degli uomini gli anniversari sollecitano riflessioni e bilanci. Nel nostro caso la scelta di legare insieme le due ricorrenze rispecchia pienamente il legame naturale che esiste tra Costituzione e processo penale[3]. Ogniqualvolta si riflette sulle regole che lo governano, anche per come declinate dalla clinica giurisprudenziale, si è chiamati inevitabilmente a misurarsi con i principi e le regole contenute nella nostra Legge fondamentale.

Non sono poche, difatti, le disposizioni della Carta riguardanti il processo penale. Alcune se ne occupano in maniera diretta, disegnando la struttura di questo delicatissimo strumento cognitivo e delineando la fisionomia dei soggetti che ne sono gli interpreti. Altre di riflesso, fornendo tutela ad una serie di diritti che possono essere limitati nel corso del processo: diritti fondamentali, o meglio, diritti inviolabili per rimanere maggiormente fedeli alle disposizioni costituzionali che li tutelano[4].

Negli artt. 13, 14 e 15 Cost., alla proclamazione di "principio" della intangibilità della libertà personale, di domicilio e delle comunicazioni segue una articolata disciplina che si fa carico di indicare le condizioni minime per tollerare atti invasivi di queste libertà. Eventualità che si presentano con una certa frequenza nel corso del giudizio penale ove, per soddisfare esigenze processuali, si finisce per conculcare proprio questi diritti fondamentali.

Le modalità di intrusione nelle libertà tutelate costituzionalmente sono naturalmente figlie dei tempi e delle tecniche che l'evoluzione

---

[3] Per i legami tra Costituzione e processo penale si vedano, tra gli altri, i contributi contenuti in Aa. Vv., *Processo penale e costituzione*, a cura di F.R. Dinacci, Milano, 2011; Aa. Vv., *Fisionomia costituzionale del processo penale*, a cura di G. Dean, Torino, 2007. Per un contributo sul tema con riferimento al precedente codice di rito si veda G. Conso, *Costituzione e processo penale*, Milano, 1969.

[4] Sulla genesi dei diritti fondamentali si veda da ultimo V. Baldini, *"Che cosa è un diritto fondamentale". La classificazione dei diritti fondamentali. Profili storico-teorico positivi*, in www.dirittifondamentali.it, 15 giugno 2016.

scientifica è in grado di mettere a disposizione dei soggetti processuali che sono chiamati a svolgere attività di carattere investigativo[5].

I nuovi strumenti di controllo informatico, che possiedono una forte capacità di intrusione nella sfera privata di ogni individuo, anche estraneo alla vicenda processuale, ne costituiscono l'esempio paradigmatico.

Proliferano forme di invasività dematerializzate della sfera personale, ma non per questo meno pericolose[6]. L'esistenza di un mondo virtuale nel quale ognuno di noi vive, lavora e "sviluppa" la propria personalità ha stimolato la nascita di forme di controllo che non investono più la persona nella sua dimensione corporale e materiale, ma in quella più impalpabile della sua estensione digitale.

Tale attenzione è d'altra parte comprensibile. Le reti informatiche, in virtù della loro natura, sono divenute anche canali utilizzati dalla criminalità, e, per questo, oggetto di attenzione da parte di coloro ai quali spetta istituzionalmente la repressione penale.

La nascita e lo sviluppo di indagini informatiche, soprattutto di carattere occulto, pongono, tuttavia, agli interpreti quesiti ai quali non è sempre facile fornire risposta.

Tra questi, il più importante è costituito dallo stabilire quali siano i limiti a cui devono soggiacere poteri così pervasivi degli organi inquirenti.

Limiti che devono certamente sussistere in quanto anche nel mondo virtuale ad ogni persona deve essere riconosciuto uno spazio che sia immune da interferenze esterne.

La ragione è abbastanza evidente. Nella rete informatica si comunica, si possono depositare documenti "personali", si può "navigare"

---

[5] Per uno sguardo d'insieme al tema si vedano S. Aterno, Digital forensics *(investigazioni informatiche)*, in *Dig. disc. pen*., Agg. VIII, Torino, 2014, p. 217 ss.; G. Di Paolo, *Prova informatica (dir. proc. pen.)*, in *Enc. dir*. annali, VI, Milano 2016, p. 739; L. Luparia, Computer crimes *e procedimento penale*, in *Modelli differenziati di accertamento*, a cura di G. Garuti, t. I, Torino, 2011, p. 396 ss.; S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 121 ss.

[6] Sulla "incapacità" del legislatore di regolare tempestivamente questo nuovo fenomeno si veda M. Daniele, *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. pen e giust*., 5, 2018, p. 831 ss.

esponendosi allo sguardo occulto altrui, insomma si possono compiere una serie di attività che forniscono informazioni sulla personalità di un individuo, molte delle quali afferenti alla dimensione più intima.

Ed allora si comprende bene come appare indefettibile misurarsi con le garanzie riconosciute dalla Costituzione ed in particolare con la tutela che la stessa offre ai diritti inviolabili dell'uomo.

2. L'inviolabilità dei diritti fondamentali: una categoria da rivitalizzare.

Ogniqualvolta si affronta il tema della tutela apprestata dalla nostra Carta fondamentale alle libertà individuali si è soliti dare maggior risalto alle garanzie (della riserva di legge e di "giurisdizione") che la stessa impone di rispettare per introdurre eventuali atti limitativi di queste libertà, mentre minore attenzione viene riservata alla circostanza che questi diritti siano stati qualificati inviolabili. Questo approccio rischia di fornire una visione errata del livello di tutela che i Costituenti hanno inteso attribuire a questi diritti, non potendo essere priva di significato la circostanza che agli stessi, ed in particolare a quelli regolati dagli artt. 13,14, 15 e 24 Cost. sia stato riconosciuto il carattere dell'inviolabilità[7].

[7] Ben altra è più complessa questione è se i diritti inviolabili ai quali fa riferimento l'art. 2 Cost. siano solo quelli previsti esplicitamente o implicitamente dalla Costituzione o se si possa fare riferimento anche a diritti desumibili da fonti esterne alla stessa: tema che l'economia del presente lavoro non consente di affrontare con la necessaria attenzione; per le varie posizioni assunte in dottrina si rimanda alla ricostruzione compiuta da A. Baldassarre, voce *Diritti inviolabili*, in *Enc. giur. Treccani*, X, Roma, 1989, p. 18 ss.; più di recente S. Mangiameli, *Il contributo dell'esperienza costituzionale italiana alla dommatica europea della tutela dei diritti fondamentali*, in *Corte costituzionale e processo costituzionale*, a cura di A. Pace, Milano, 2006, p. 471 ss. Di recente si è osservato come l'annosa *querelle* sul catalogo aperto o chiuso dei diritti fondamentali potrebbe essere considerato anche come un falso problema, cfr. G. Silvestri, *L'individuazione dei diritti della persona*, in www.penalecontemporaneo.it, 27 ottobre 2018, p. 2, in quanto «la struttura delle norme costituzionali in generale, e di quelle di principio in specie, è talmente ampia da adattarsi incessantemente al mutare dei tempi e da consentire, come naturali sviluppi, nuove interpretazioni e nuove applicazioni, in risposta a nuovi pericoli e nuove esigenze sorti in tempi successivi all'entrata in vigore della Costituzione».

Per rimanere aderenti alla lettera ed allo spirito della Carta occorre, dunque, confrontarsi necessariamente con questo speciale attributo.

Come si è osservato in dottrina, tradizionalmente, il concetto di inviolabilità è stato usato in «relazione ai "diritti dell'uomo e del cittadino" con particolare riferimento all'impossibilità giuridica dei poteri pubblici di eliminarli, in tutto o in parte dall'ordinamento costituzionale positivo o, più semplicemente, di comprimerli sostanzialmente»[8].

Per comprendere il reale valore di questo carattere torna poi utile anche considerare quella particolarissima tradizione che conduceva a qualificare come inviolabile innanzitutto la persona del monarca, come anche gli altri organi supremi dello Stato per «collocarli giuridicamente al di fuori di ogni valutazione politica e financo di ogni discussione»: simboleggiandone così la supremazia giuridica e valoriale. Questa tradizione ha influenzato i sistemi liberal-democratici ottocenteschi che hanno utilizzato la stessa espressione per connotare alcuni principi astratti a fondamento delle nuove forme statuali, attribuendola in particolare ai c.d. diritti dell'uomo.

La stessa tradizione ha condizionato anche la nostra Costituzione, dove la scelta di assegnare ad alcune libertà individuali il carattere della inviolabilità può essere letta come espressiva della chiara volontà di attribuirgli un primato valoriale. Come efficacemente è stato sottolineato, nell'assetto della nostra Carta emerge «un significato complessivo dei diritti inviolabili che li identifica con i valori originari, assolutamente primari e perciò intangibili nel loro nucleo assiologico, sia da parte di qualsiasi soggetto privato ... sia da parte di qualsiasi potere costituito»[9].

Questi diritti si pongono allora quale fondamento del nostro sistema di valori costituzionale e di quel modello di convivenza civile ideato e voluto dalla Legge fondamentale. Dunque i diritti inviolabili come connotativi della nostra Costituzione e della forma di democrazia

---

[8] V. A. Baldassarre, voce *Diritti inviolabili*, *Enc. giur. Treccani*, X, Roma, 1989, p. 27, dal quale sono tratte anche le citazioni che seguono nel testo. In tema si veda anche F. Grossi, *Introduzione ad uno studio sui diritti inviolabili nella Costituzione italiana*, Padova, 1972.

[9] V. A. Baldassarre, voce *Diritti inviolabili*, cit., p. 29.

pluralista in essa previsto[10]. Ma come osservato sarebbe riduttivo intendere la inviolabilità come equivalente di irrivedibilità consegnando così questa categoria alla sola dimensione formalistica e legalitaria. In questo modo si finirebbe per svilire il significato più profondo della qualificazione di inviolabilità di alcuni diritti «e cioè il fatto che sono essi a costituire la misura di valore della democrazia, e non viceversa, e che è il loro rispetto a contrassegnare primariamente la "legittimità" dell'azione della maggioranza e delle decisioni di questa e non viceversa»[11].

Sulla base di queste considerazioni si giunge così ad una prima conclusione: con la qualificazione di inviolabilità emerge la peculiarità connotativa, dal punto di vista costituzionale, di alcuni diritti, perché, se è vero che la Carta non ha predisposto una «completa o assoluta gerarchia di valori [...] non è men vero che ha inteso porre alcuni valori o alcuni principi al di sopra di altri»[12].

Rispecchiano il precipuo rilievo attribuito ai diritti inviolabili le garanzie che li corredano. Per quel che qui interessa nel caso delle c.d. libertà negative, in particolare la libertà personale, di domicilio e delle comunicazioni, la Carta, nonostante non fissi limiti di valore, prevede alcune specifiche garanzie procedurali che debbono essere rispettate qualora si vogliano imporre eventuali restrizioni materiali. Un riconoscimento che si può considerare un'ammissione implicita che anche questi diritti non siano immuni da possibili limitazioni esterne[13].

---

[10] Come osservava P. Calamandrei nella prefazione alla seconda edizione di F. Ruffini, *Diritti di libertà*, Firenze, 1946, ora in P. Calamandrei, *L'avvenire dei diritti di libertà*, Giulianova, 2018, p. 58, «in un ordinamento democratico le libertà individuali, anche se non fossero reclamate dai singoli a difesa dell'interesse privato, apparirebbero come primordiale esigenza dell'interesse pubblico: perché di esse la democrazia ha bisogno per respirare, ossia per vivere»

[11] V. A. Baldassarre, voce *Diritti inviolabili*, cit., p. 30, il quale osserva altresì che l'integrale riduzione della problematica della legittimità a quella della legalità, implicita nell'identificazione tra inviolabilità e irrivedibilità, «fa perdere alla dichiarazione dell'art. 2 Cost. una parte sostanziale del suo più significativo spessore».

[12] Cfr. A. Baldassarre, op. cit., p. 31.

[13] Come osserva tuttavia G. Amato, *Individuo e autorità nella disciplina della libertà personale*, Milano, 1967, p. 323, l'inviolabilità si traduce nell'attribuzione alla libertà inviolabile «di una tendenziale priorità sui rispettivi limiti che

Questa tessitura riflette la trama semantica in cui si sviluppa il concetto moderno di libertà: un orizzonte di negazione, come ha osservato un filosofo contemporaneo[14]. Una dimensione, quella contemporanea e liberale, non priva di ambiguità poiché, come già aveva colto Nietzsche, in una delle sue opere più interessanti: «le istituzioni liberali cessano di essere liberali non appena si riesce ad ottenerle: non v'è nulla in seguito, che in maniera più grave e radicale delle istituzioni liberali danneggi la libertà»[15]. Una lezione che sarà poi ripresa e sviluppata da Foucault, nei suoi seminari parigini degli anni settanta, laddove il filosofo francese analizzando le dinamiche di libertà delle democrazie "liberali" mette in evidenza come le stesse abbiano bisogno di libertà, la promettono, la organizzano, ma allo stesso tempo gestendone in forma capillare le procedure, la limitano sino al rischio dell'annullamento: «la nuova arte di governo che si è formata nel XVIII secolo, racchiude in sé, nel suo stesso cuore, un rapporto di produzione/distruzione [con] la libertà [...] Da un lato, dunque occorre produrre la libertà, ma questo stesso gesto implica, dall'altro, che si stabiliscano delle limitazioni, dei controlli delle coercizioni, delle obbligazioni sostenute da minacce, e così via»[16].

Pur muovendosi in questo orizzonte di riconoscimento/ negazione/ limitazione, dalla nostra Carta e soprattutto dalla qualificazione di inviolabilità si possono trarre, anche per quanto appena osservato, delle importanti implicazioni.

---

impone di preferirla a questi ultimi nelle ipotesi di dubbio, sia evitandone il sacrificio quando sia questo il *thema decidendum*, sia, ad un diverso livello fornendole il più efficiente degli strumenti di tutela fra quanti ne offre volta a volta l'ordinamento».

[14] V. R. Esposito, *Politica e negazione. Per una filosofia affermativa*, Torino, 2018, p. 95, il quale sottolinea altresì come questa declinazione negativa del concetto di libertà, quale assenza di restrizioni e costrizioni viene per la prima volta esplicitata da Jeremy Bentham, portando alle estreme conseguenze una linea di pensiero che «originata da Hobbes, diventa largamente prevalente nella filosofia politica moderna».

[15] Cfr. F. Nietzche, *Crepuscolo degli idoli*, in *Opere*, a cura di G. Colli e M. Montinari, Vol. VI, t. III, Milano, 1991, p. 113.

[16] Cfr. M. Foucault, *Nascita della biopolitica. Corso al College de France* (1978/1979), Milano, 2005, p. 66.

Se limiti alle libertà inviolabili, ed in particolare alle libertà individuali, sono possibili non si può ammette che il legislatore sia del tutto libero nella loro previsione[17].

Tale ultima considerazione merita di essere chiarita. Come sottolineato da attenta dottrina le restrizioni ai diritti inviolabili possono essere previste a condizione che le stesse siano giustificate dal soddisfacimento di doveri inderogabilmente fissati dalla Costituzione e rispettando il bilanciamento con altri valori pari ordinati[18].

Quest'ultima operazione risulta tuttavia tutt'altro che agevole[19] e non priva di pericoli per la tenuta della garanzia[20], tanto da provocare in tutte le esperienze giuridiche degli ordinamenti democratici la creazione di formule giuridiche volte a contenere gli spazi all'interno dei quali far oscillare i termini del bilanciamento.

Vari gli strumenti che sono stati creati in proposito: da quello di "contenuto essenziale" del diritto, caro alla dottrina di matrice tedesca e che raccoglie proseliti anche in quella italiana, sino alla "garanzia dell'istituto" o alle "garanzie istituzionali" [21]. Ognuno di questi concetti è portatore della propria verità e capace, se ben utilizzato, di divenire strumento utile sia per ricostruzione logica dei vari tipi di garanzie sia per la risoluzione pratica di alcuni delicati problemi.

Al di là di tali rilevantissime questioni ciò che qui preme ribadire, e che assume maggior rilievo per la nostra indagine, è la forza contenitiva che il riconoscimento dell'inviolabilità di un diritto esercita nei confronti del legislatore ordinario, al quale non può essere attribuita una assoluta libertà nel dettare previsioni limitative di diritti che si caratterizzano per questo attributo costituzionale.

---

[17] Sul tema C. Mortati, *Istituzioni di diritto pubblico*, II, 8° ed., Padova, 1969, p. 950 ss.

[18] Cfr. L. Elia, *Le misure di prevenzione fra l'art. 13 e l'art. 25 della Costituzione*, in *Giur. cost*., 1964, p. 940 e ss.

[19] È tutt'altro che agevole difatti individuare in base a quali regole giuridiche si possa operare questo bilanciamento.

[20] Il giudizio di bilanciamento potrebbe di fatto condurre ad uno svuotamento della garanzia della inviolabilità.

[21] Cfr. A. Baldassarre, voce *Diritti inviolabili*, cit., p. 32, al quale si rimanda anche per l'illustrazione di ognuno di questi strumenti.

Si è già avuto modo di metterlo in evidenza: limiti a diritti inviolabili sono costituzionalmente tollerabili a condizione che abbiano una base in altri valori costituzionalmente previsti, al fine di tutelare altro diritto inviolabile o rendere possibile l'adempimento di un dovere inderogabile.

Nel far questo il legislatore è sottoposto tuttavia al principio della coessenzialità o della necessarietà del limite[22]. Per dirla in maniera più chiara, per l'imposizione di un limite ad un diritto inviolabile, non è sufficiente che si possa individuare un legame giustificativo (ragionevolezza, proporzionalità) con altro valore costituzionale, in potenza limitativo del c.d. contenuto essenziale di quel diritto, ma che tale relazione giustificativa sia per così dire rafforzata dalla circostanza che in carenza di quel limite, il valore costituzionale che lo legittima risulterebbe sostanzialmente leso o violato[23]. Solo così si rimane fedeli al valore primario che, con il riconoscimento della inviolabilità, i Costituenti hanno voluto attribuire ad alcuni diritti.

3. Indagini informatiche e tutela dei diritti inviolabili.

Le precedenti considerazioni tornano utili per affrontare le questioni legate ai diversi problemi interpretativi che nascono dall'uso sempre più massivo delle indagini informatiche ed in particolare di quelle che vengono svolte mediante il c.d. *trojan horse*.

Come a tutti noto si tratta di una tecnica investigativa che permette, mediante l'invio di un *malicious software* in un dispositivo elettronico (*computer, smartphone, tablet* etc.), di compiere attività di ricerca e di sorveglianza *online* su quest'ultimo[24].

---

[22] V. in proposito A. Baldassarre, voce *Diritti inviolabili*, cit., p. 37.

[23] Si vedano al riguardo le considerazioni di M. Luciani, *La produzione economica privata nel sistema costituzionale*, Padova, 1983, p. 63. Sui limiti che deve incontrare il legislatore ordinario nella previsione di limiti a diritti di cui agli artt. 13, 14 e 15 Cost. si veda anche R. Fonti, *La tutela costituzionale delle libertà individuali*, in *Fisionomia costituzionale del processo penale*, a cura di G. Dean, Torino, 2007, p. 11.

[24] Per un quadro d'insieme delle caratteristiche anche tecniche di questo nuovo strumento investigativo si veda R. Brighi, *Funzionamento e potenzialità*

Con questo accesso occulto, fisico o da remoto[25], è possibile appropriarsi non solo di tutto quanto contenuto nel dispositivo *target* (*online search*), ma anche di carpire, in tempo reale, tutte le attività che con lo stesso possono essere compiute, accedendo anche ai suoni ed alle immagini captati con l'attivazione dei dispositivi audio o video del *target* (*online surveillance*) [26].

Non vi è necessità di impiegare molte parole per dimostrare la pervasività di un tale strumento e soprattutto la sua enorme, quanto sinora sconosciuta, capacità intrusiva nella intimità di una persona[27].

Il c.d. captatore informatico è in grado di raccogliere, peraltro in tempo reale, una mole di informazioni su ogni aspetto della vita di un soggetto, da quella privata a quella lavorativa, che non ha sicuramente precedenti. Nei nostri *smartphone* è contenuta e filtrata la nostra intera esistenza.

Il primo tema che merita di essere trattato è se questa nuova tecnica investigativa comporti la violazione di uno, o più, dei diritti inviolabili tutelati dagli artt. 13, 14 e 15 Cost.

Per rispondere a tale quesito occorre partire da una premessa.

In carenza di una disciplina organica della materia, per individuare quale potesse essere quella applicabile al c.d. captatore informatico si sono sinora presi in considerazione soltanto alcuni usi del *maleware*[28]. Un esempio tipico di questo modo di procedere lo si

---

investigative del malware, in *Nuove norme in tema di intercettazioni*, a cura di G. Giostra e R. Orlandi, Torino, 2018, p. 211 ss.

[25] L'inoculamento del captatore in un dispositivo-*target* può avvenire di fatto in due maniere: 1) agendo direttamente sullo stesso qualora se ne abbia la disponibilità fisica o 2) a distanza servendosi di un qualunque *file* ingannevole, che aperto dall'utente installa il *trojan* ivi mascherato.

[26] Su questa distinzione si veda M. Griffo, *Una proposta costituzionale per arginare lo strapotere del captatore*, in *Diritto penale contemporaneo*, 2, 2018, p. 24 ss.

[27] Le numerose funzioni del captatore sono ben elencate da F. Caprioli, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. Bras. Direito Proc. Pen.*, 2017, 2, p. 483.

[28] Ad avviso di F. Caprioli, *Il "captatore informatico"*, cit., p. 486, la circostanza che non vi sia una specifica regolamentazione non può condurre a ritenere che queste attività investigative siano per ciò solo vietate, poiché in alcuni casi sono riconducibili a mezzi di ricerca della prova già disciplinati

può trovare nella recente decisione delle Sezioni unite Scurato nella quale l'attenzione dei giudici del Supremo collegio si è concentrata principalmente sulla verifica di quale potesse essere la disciplina applicabile alle video riprese eseguite mediante l'uso del captatore, non occupandosi delle altre[29].

Questa scelta, tuttavia, finisce per eludere il tema più importante posto dal nuovo strumento investigativo: il suo corretto inquadramento.

L'attivazione di una *web camera*, mediante *trojan*, è solo una delle tante funzioni che con questo mezzo si possono attivare, ve ne sono altre che sicuramente non possono essere considerate come intercettazioni e che allo stesso tempo appare difficile classificare tra gli strumenti investigativi attualmente disciplinati dal codice di rito.

Si pensi, a titolo esemplificato, alle indagini volte a ricavare copia, parziale o totale dell'*hard disk* trasmettendo così agli inquirenti dati ed informazioni in tempo reale con l'attivarsi di una connessione *internet*[30].

---

ed in secondo luogo perché nel nostro sistema processuale sono ammissibili anche le prove atipiche.

[29] Cfr. Cass., Sez. un. 28 aprile 2016, n. 26889, Scurato, in *Arch. n. proc. pen*., 2017, p. 76 ss., con nota di A. Camon, *Cavalli di Troia in Cassazione*; in Cass. pen., 2016, p. 2274, con nota di A. Balsamo, *Le intercettazioni mediante* virus *informatico tra processo penale italiano e Corte europea*; in *Proc. pen. giust*., 2016, fasc. 5, p. 21, con nota di P. Felicioni, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*; in www.penalecontemporaneo.it, 20 marzo 2017, con nota di L. Giordano, *Dopo le sezioni unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*. In tema si vedano altresì A. Gaito-S. Furfaro, *Le nuove intercettazioni ambulanti: tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza della collettività*, in *Arch. pen*., 2016, II, p. 309; A. Cisterna, *Spazio ed intercettazioni, una* liaison *tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite*, in *Arch. pen*., II, p. 331; L. Filippi, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico)*, in *Arch. pen*., 2016, II, p. 348; L. Picotti, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. pen*., 2016, II, p. 354; G. Lasagni, *L'uso di captatori informatici (*trojans*) nelle intercettazioni "fra presenti"*, in www.penalecontemporaneo, 7 ottobre 2016.

[30] Analoghe difficoltà si possono trovare anche per la qualificazione della captazione della navigazione dell'utente il cui *target* viene monitorato.

Per le c.d. perquisizioni *online*[31], come osservato in dottrina e giurisprudenza, appare veramente arduo poter ricondurre la ricerca occulta, così operata, nei paradigmi normativi esistenti, ossia nelle disposizioni che regolano la c.d. perquisizione ordinaria (artt. 247-252 c.p.p.), o in quelle previste per la c.d. perquisizione informatica regolata dall'art. 247 comma 1*bis* c.p.p.[32]

Molte sono difatti le ragioni, o meglio le differenze, che non consentono un tale inquadramento. Le ricerche condotte per il tramite del captatore sono, difatti: occulte, permanenti e capaci di raccogliere una mole indifferenziata di dati.

Le difficoltà, e talvolta l'impossibilità, di ricondurre nelle discipline già esistenti (ossia perquisizione, ispezione ed intercettazioni) le attività investigative di fatto compiute attraverso l'attivazione delle diverse funzioni del *trojan horse* impone, o meglio, rende imprescindibile verificare se queste attività si pongano in contrasto con diritti costituzionalmente tutelati ed in particolare con quelli inviolabili, per le cui limitazioni è imposto il rispetto della riserva di legge e l'attribuzione all'autorità giudiziaria dell'adozione dei relativi atti.

---

[31] Con questa espressione, in realtà, come osservato da L. Parlato, *Problemi insoluti: le perquisizioni* on-line, in *Nuove norme in tema di intercettazioni*, a cura di G. Giostra e R. Orlandi, Torino, 2018, p. 295, si intende fare riferimento a quelle operazioni eseguite mediante *trojan* che non possono essere ricondotte al concetto di intercettazione ossia a quelle operazione compiute «all'insaputa dell'interessato, volte ad esplorare un sistema informatico per trarne utili elementi probatori, sia a monitorarlo con costanza», sottolineando altresì che non deve trarre in inganno l'uso della parola "perquisizioni" nella denominazione in quanto rispetto all'istituto già esistente «questo è di gran lunga più invasivo».

[32] Così espressamente F. Caprioli, *Il "captatore informatico"*, cit., p. 489. Si vedano al riguardo anche le considerazioni di P. Bronzo, *L'impiego del* trojan horse *informatico nelle indagini penali*, in *Riv. it. scienze giur.*, 2017, p. 347; M. Daniele, *Contrasto al terrorismo e captatori informatici*, in *Riv. dir. proc.*, 2017, p. 403; A. Testaguzza, *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. pen. proc.*, 2014, p. 759; M. Trogu, *Sorveglianza e "perquisizioni" online su materiale informatico*, in *Le indagini atipiche*, a cura di A. Scalfati, Torni, 2014, p. 444. In giurisprudenza Cass., Sez. IV, 17 aprile 2012, n. 19618, in *Cass. pen.*, 2013, p. 1523 con nota di G. Bono, *Il divieto di indagini* «ad explorandum» *include i mezzi informatici di ricerca della prova*.

Il problema non è stato affrontato neppure dalla recente legge di riforma delle intercettazioni, non ancora entrata in vigore, poiché la stessa si è limitata a regolare le sole attività di intercettazione realizzate tramite il *virus* informatico, e più precisamente quelle audio e di carattere ambientale, ottenute mediante l'inserimento di un *trojan* ed esclusivamente in dispositivi portatili[33], senza peraltro prendere in considerazione l'utilizzo del nuovo insidiosissimo strumento in relazione a dispositivi fissi: come il *computer* ad esempio[34].

L'assenza di una disciplina organica del nuovo strumento appare pericolosissima poiché in virtù delle diverse funzioni attivabili mediante captatore informatico vi è una estrema facilità, nonostante si attivi una sola funzione, che le attività acquisitive possano passare la misura, con la conseguenza che «gli impieghi *contra legem* sono solo limitatamente controllabili da parte del giudice, del pubblico ministero, della stessa polizia giudiziaria»[35].

Anche per queste ragioni si deve sondare la possibilità di procedere ad una autonoma qualificazione del nuovo strumento investigativo, e non limitarsi ad isolare la singola funzione, che sembra essere l'approccio sin qui seguito anche dalla giurisprudenza, che da un lato ha posto grande attenzione nel trovare la disciplina applicabile nell'ipotesi in cui mediante il *trojan* si captino "comunicazioni", ma non si è tuttavia misurata, con

---

[33] Ci si riferisce alla d. lgs. n. 216/2017. In particolare per quel che riguarda il captatore le nuove disposizioni troveranno applicazione per le «operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 marzo 2019», secondo quanto stabilisce la disposizione transitoria di cui all'art. 9 comma 1, come modificato dal d.l. n. 91/2018, conv. nella l. n. 108/2018. Con legge n. 145 del 2018 (legge di bilancio) l'entrata in vigore è stata prorogata al 1° agosto 2019, termine ulteriormente differito al 1° gennaio 2020, per effetto dell'art. 9, c. 2, del d.l. n. 53/2019. Con specifico riferimento alla disciplina del captatore si deve poi segnalare come la stessa sia stata anche oggetto di interpolazione ad opera della l. n. 3/2019 (c.d. legge spazza-corrotti).

[34] In tema si vedano le considerazioni di L. Parlato, *Problemi insoluti*, cit., p. 289 ss., la quale osserva anche che «il lato "nascosto", su cui la novella è rimasta silente, crea difficoltà interpretative ancora maggiori di quelle direttamente legate ala lettura del testo».

[35] V. P. Bronzo, *Intercettazioni ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in *Nuove norme in tema di intercettazioni*, a cura di G. Giostra e R. Orlandi, Torino, 2018, p. 239. In tema si vedano anche le considerazioni di A. Camon, *Cavalli di Troia*, cit., p. 96.

analogo rigore, con quei casi in cui mediante intrusore ci si appropri del contenuto di un *computer*[36].

Così facendo, a mio avviso, si finisce per non cogliere le peculiarità e le caratteristiche del nuovo strumento investigativo, così altamente invasivo e, soprattutto, non si offrono delle risposte interpretative veramente soddisfacenti.

Ed ancora, ciò che in sede speculativa non si è considerato con la dovuta attenzione è se la stessa intrusione che si opera mediante captatore debba essere oggetto di una autonoma valutazione giuridica.

Questa maniera di non considerare affatto l'immissione occulta in un sistema informatico sembra riecheggiare l'approccio adottato in materia di intercettazioni, dove non si è tenuta mai nella dovuta considerazione la circostanza che per posizionare delle microspie in una abitazione fosse necessario accedervi clandestinamente; mostrando così scarsa sensibilità per quanto impone l'art. 14 Cost.[37].

Per non dimostrarsi altrettanto insensibili occorre verificare come possa essere valutata l'intrusione del captatore nei sistemi informatici. Un quesito che impone di considerare dove penetra questo nuovo strumento investigativo.

Coglie a mio avviso nel segno il rilievo che quell'insieme di dati, informazioni ed attività possa essere considerata come una entità

---

[36] Cfr. Cass., Sez. V, 14 ottobre 2009, Virruso, in www.penale.it, ove si è affermato che l'acquisizione, mediante captatore, di dati a contenuto non comunicativo, non violi alcun diritto inviolabile.

[37] Secondo la giurisprudenza maggioritaria la collocazione di microspie in un luogo di privata dimora, costituendo una modalità attuativa delle intercettazioni si deve considerare ammessa dalla legge, così tra le ultime, Cass. Sez. II, 13 febbraio 2013, n. 21644, in CED Cass., n. 255541, con la quale è stata anche dichiarata la manifesta infondatezza della questione di legittimità costituzionale dell'art. 266 comma 2 c.p.p., per violazione dell'art. 14 Cost.; Cass., Sez. VI, 25 settembre 2012, n. 41514, in CED Cass., n. 253805, ove si è sottolineato che il pubblico ministero, nel suo provvedimento non è tenuto a precisare le modalità di intrusione delle microspie. In dottrina in senso critico A. Camon, *Le intercettazioni nel processo penale*, Milano, 1996, p. 197, più recentemente A. Capone, *Intercettazioni e costituzione. Problemi vecchi e nuovi*, in *Cass. pen.*, 2017, p. 1267, il quale sottolinea che «l'art. 14 Cost. imponga al legislatore di circoscrivere almeno dall'esterno l'ambito entro cui questo tipo di attività, naturalmente segrete, risulta consentito»

complessa ovvero come una realtà unitaria alla quale possa essere riconosciuta la qualifica di domicilio, o, per dirla meglio, di domicilio informatico[38].

Nonostante siano state espresse alcune perplessità in dottrina su questa possibilità vi sono buoni argomenti per sostenere un simile inquadramento[39].

Per far questo occorre muovere dal significato che la Costituzione ha inteso dare al domicilio per come lo stesso è filtrato dai lavori preparatori.

Emerge da questi ultimi che nel concetto di domicilio si volevano far rientrare non solo l'abitazione e i luoghi a questa assimilabili, ma ogni luogo di cui si dispone a titolo privato e nel quale non necessariamente si svolgono attività domestiche[40].

Ed ancora, come non si è mancato di riconoscere negli stessi anni in cui vedeva la luce la nostra Carta fondamentale, il domicilio è stato tutelato in maniera così forte in quanto costituisce una proiezione spaziale della persona, secondo la famosissima definizione di Amorth[41]. Una stessa impostazione che riguarda anche il diritto alla segretezza delle comunicazioni tutelato costituzionalmente in quanto proiezione, in questo caso spirituale, di ogni individuo[42]. Queste disposizioni, per dirla con la Corte suprema statunitense «*protectes people, not pleace*»[43].

---

38 Si vedano al riguardo S. De Flammineis, *Le intercettazioni telematiche*, in *Dir. pen. proc*., 2013, p. 989; S. Signorato, *Modalità procedimentali dell'intercettazione tramite captatore informatico*, in *Nuove norme in tema di intercettazioni*, a cura di G. Giostra e R. Orlandi, Torino, 2018, p. 263 ss.; M. Torre, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. proc*., 2015, p. 1168-1170.

39 Esprime perplessità A. Capone, *Intercettazioni e costituzione*, cit., p. 1266, ritenendo questa strada «un poco accidentata».

40 Per la ricostruzione dei lavori preparatori dell'art. 14 Cost. v. G. Amato, sub *artt. 13-14 Cost*., in *Commentario della Costituzione*, a cura di G. Branca, *Rapporti civili*, Roma-Bologna, 1977, p. 57.

41 Cfr. A. Amorth, *La Costituzione italiana*, Milano, 1948, p. 62.

42 V. F. Bricola, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen*., 1967, p. 1120.

43 Citata in C. Pinelli, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite* "virus *di Stato"*, in *Dir. pen. cont*., 4, 2017, p. 82.

Dunque il domicilio, dal punto di vista costituzionale coincide con un luogo del quale si ha la disponibilità ed il correlato potere di escludere altri, e che viene tutelato proprio in quanto in esso si ha una proiezione della persona.

Non vi è alcun dubbio che sin qui il concetto di luogo è stato inteso in senso fisico, ma ciò non osta a che questo concetto possa essere trasfigurato seguendo la *ratio* ispiratrice, o meglio il significato essenziale, che connota la tutela costituzionale del domicilio.

Una operazione che non ha nulla di scandaloso, in quanto come ampiamente riconosciuto, i diritti fondamentali, al pari di ogni prodotto culturale, sono sottoposti ad una naturale opera di rimodellamento evolutivo. Ai mutamenti culturali si accompagnano revisioni ampliative o meglio letture progressive che siano capaci di adattare il significato sostanziale dei diritti alle nuove esigenze di tutela[44].

Una volta individuato il nucleo fondamentale del diritto garantito dall'art. 14 Cost. nella necessità di tutelare l'individuo in quegli spazi "riservati" in cui lo stesso manifesta la propria personalità, è possibile ritenere che la tutela che la Carta fondamentale accorda al domicilio si possa estendere anche a luoghi dematerializzati, ma che costituiscono comunque uno spazio, anche solo idealmente circoscritto, in cui, al pari di quello che avviene per il domicilio fisico, si proietta la personalità di un individuo.

D'altra parte se si riflette sulla circostanza che l'idea di luogo si ricollega «a quella di spazio potenzialmente idoneo a contenere qualcosa»[45] diviene non troppo difficile qualificare l'intrusione in un qualsiasi apparecchio *target* come intrusione in domicilio informatico.

Si può allora affermare, come già fatto con efficacia, che oggi esista anche «una proiezione *informatica* dell'individuo destinata ad

---

[44] Si vedano in proposito A. Baldassarre, voce *Diritti inviolabili*, cit., p. 18 ss.; G. Silvestri, *L'individuazione dei diritti*, cit., p.3; nonché M. Luciani, *Positività e meta positività e parapositività dei diritti fondamentali*, in *Scritti in onore di L. Carlassare*, Napoli, 2009, II, p. 1067.

[45] V. S. Signorato, *Modalità procedimentali dell'intercettazione*, cit., p. 264, nota 3.

allargare i confini del diritto all'intimità della vita privata e al rispetto della dignità personale»[46].

D'altra parte questa idea di accostare quello spazio virtuale del quale ognuno di noi dispone con quella di domicilio informatico è già entrata nel nostro ordinamento se solo si considera l'inserimento nel lontano 1993 della fattispecie di accesso abusivo a sistema informatico proprio tra i delitti contro l'inviolabilità del domicilio[47]. Una collocazione che sembra voler sottolineare che anche per il legislatore i sistemi informatici possano essere considerati come altrettanti domicili.

L'uso delle parole legate alle realtà informatiche d'altronde evidenzia questo concetto di entrare in uno spazio: accedere, entrare, pass*word*, etc.

Questa possibilità tuttavia non raccoglie il consenso di tutti in dottrina.

Si è infatti osservato che sarebbe più opportuno seguire gli insegnamenti della Corte costituzionale tedesca che ha negato che la salvaguardia della "intimità informatica" possa trovare copertura costituzionale nella libertà di domicilio, ma in un autonomo diritto all'*uso riservato e confidenziale delle tecnologie informatiche* implicito nella tutela che l'art. 1 *Grundgesetz* assicura alla dignità dell'uomo[48].

Quand'anche si seguisse lo stesso percorso e si ammettesse che nell'art. 2 Cost. possa essere enucleato il nuovo diritto inviolabile alla riservatezza informatica[49], non sarebbe comunque agevole farne discendere

---

[46] Così F. Caprioli, *Il "captatore informatico"*, cit., p. 491.

[47] Ci si riferisce alla legge 23 dicembre 1993, n. 547, con la quale è stato introdotto nel codice penale l'art. 615-*ter* c.p.

[48] Ci si riferisce a Bundesverfassungsgericht, 27 febbraio 2008, in *Riv. trim. dir. pen. ec.*, 2009, p. 679; nonché più di recente, Bundesverfassungsgericht, 8 maggio 2016, in www.penalecontemporaneo.it, 8 maggio 2016, con nota di A. Venegoni-L. Giordano, *La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazione da remoto a mezzo di strumenti informatici*. In tema si veda altresì F. Nicolicchia, *I limiti fissati dalla Corte costituzionale tedesca agli strumenti di controllo tecnologico occulto: spunti per una trasposizione nell'ordinamento italiano*, in www.archiviopenale.it, 2017.

[49] Come auspica R. Orlandi, *Osservazioni sul documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in www.

il rispetto della doppia riserva imposta dalla Costituzione solo per gli artt. 13, 14 e 15 Cost.[50]

Questo diritto alla riservatezza informatica secondo altra parte della dottrina si deve comunque considerare tutelato dall'art. 8 della Convenzione europea il quale riconosce che «ogni persona ha il diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza», operante nel nostro sistema per effetto dell'art. 117 Cost.[51]. Una disposizione che è stata interpretata dalla Corte EDU in maniera estensiva tanto da ricomprendervi non solo il diritto alla riservatezza, ma anche quello alla autodeterminazione informatica[52]. Interferenze nella vita privata possono sussistere, *ex* art. 8, par. 2, sempre che abbiano una base legale ed allo stesso tempo che siano necessarie, in una società democratica, alla tutela di alcuni valori fondanti dei singoli ordinamenti[53].

In qualche modo alle stesse conclusioni si giunge seguendo l'impostazione che preferisco: ossia che ogni dominio informatico

---

archiviopenale.it, 25 luglio 2016; Id., *La riforma del processo penale fra correzioni strutturali e tutela progressiva dei diritti fondamentali*, in *Riv. it. dir. proc. pen*., 2014, p. 1133.

50 Difficoltà evidenziata anche da F. Iovene, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze dell'accertamento penale*, in *Dir. pen. cont*., *Riv. trim*., 2014, p. 336, nonché da P. Bronzo, *L'impiego del* trojan horse, cit., p. 349.

51 Su questa necessità si veda G. Illuminati, *La tutela della segretezza delle comunicazioni tra vecchio e nuovo codice*, in *Processo penale e valori costituzionali nell'insegnamento di Vittorio Grevi*, Padova, 2013, p. 106; R. Orlandi, *La riforma del processo penale*, cit., p. 1154; P. Felicioni, *L'acquisizione da remoto di dati digitali*, cit., p. 125; F. Iovene, *Le c.d. perquisizioni* online, cit., p. 336; G. Lasagni, *L'uso dei captatori informatici (*trojans*) nelle intercettazioni tra presenti*, in www.penalecontemporaneo.it, 7 ottobre 2016, p. 15 ss. Ad avviso di L. Parlato, *Problemi insoluti*, cit., p. 289 ss., p. 300 ss., la varietà di ricerche che è possibile fare mediante captatore informatico implica che siano invocabili le garanzie offerte da una serie di disposizioni costituzionali a tutela delle libertà individuali (artt. 13, 14, 15 Cost.) e dalle fonti europee.

52 Si veda in proposito Corte edu, Sez. V, 2 settembre 2010, Uzun c. Germania. Sulla circostanza che anche il controllo della navigazione *online* interferisca con il diritto della persona al rispetto della propria vita privatasi veda Corte edu, Sez. IV, 3 aprile 2007, Copland c. Regno Unito.

53 V. A. Galluccio, *Profili generali sugli artt. 8-11*, in *Corte di Strasburgo e giustizia penale*, a cura di G. Ubertis e F. Viganò, Torino, 2016, p. 257-261.

costituisca un domicilio che deve essere tutelato secondo quanto prevede l'art. 14 Cost.

Mi preme sul punto fare una precisazione. Questo inquadramento porta con sé una conseguenza: la necessità che il legislatore tenga conto della natura inviolabile del diritto in questione. Come già messo in luce, quando ci si misura con un diritto inviolabile è indispensabile che il legislatore rispetti il principio della coessenzialità o necessarietà del limite e per far questo, ossia per introdurre misure limitative di questi diritti, si deve trovare una ragione giustificatrice dotata di un preciso fondamento costituzionale.

Non è tuttavia sufficiente invocare l'esigenza costituzionale all'accertamento dei reati, tutelata dall'art. 112 Cost., ma è necessario preventivamente dimostrare che la stessa sarebbe vanificata se non si consentissero atti limitativi della libertà inviolabile che viene in questione[54].

4. Alcune considerazioni per concludere.

Se le osservazioni sin qui svolte sono corrette appare imprescindibile la necessità di regolare normativamente tutte le attività che si compiono mediante il captatore informatico[55].

---

[54] In virtù di queste considerazioni si impone costituzionalmente la necessità che vengano adottate discipline positive decisamente articolate dalle quali traspaia che si sia fatto buon uso del principio appena richiamato nel testo. Sin qui la dottrina ha invocato la necessità che quando si intervenga su diritti fondamentali si debba far uso del principio di proporzionalità, la cui più compiuta elaborazione si deve alla dottrina tedesca e che ha raccolto numerosi consensi anche in quella italiana, v. R. Orlandi, *La riforma del processo penale*, cit., p. 1157; per considerazione espresse in relazione al tema che qui interessa si veda G. Lasagni, *L'uso dei captatori informatici*, cit., p. 20 ss.; F. Nicolicchia, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in www.penalecontemporaneo.it, 8 gennaio 2018. Sulla circostanza che il principio di proporzionalità debba essere considerato come criterio informatore di ogni misura che incida negativamente sui diritti di libertà dei singoli, cfr. M. Caianello, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont*., *Riv. trim*., 2014, p. 144.

[55] Esigenza manifestata da tempo dalla dottrina italiana, a titolo esemplificativo: *Necessaria una disciplina legislativa in materia di captatori informatici (c.d.*

Una disciplina che tuttavia allo stato manca, né questa carenza, per quanto già visto, appare colmabile con l'entrata in vigore delle nuove disposizioni sulle intercettazioni telefoniche[56]. Prima di concludere non posso allora sottrarmi dall'affrontare, sia pur sinteticamente, un quesito finale.

In assenza di una espressa disciplina quale deve essere la sorte delle investigazioni informatiche compiute attraverso il c.d. *trojan horse* e non riconducibili all'interno delle discipline dettate dal codice di rito?

La questione non è delle più banali, poiché per darle risposta occorre misurarsi con uno dei temi più tormentati della procedura penale: la sorte degli atti investigativi non regolati dalla legge che violino libertà costituzionalmente tutelate.

Difatti, una volta appurato che l'intrusione mediante captatore in un apparecchio *target* nonché la maggior parte delle funzioni che poi si attivano costituiscono attività investigativa non regolata dalla legge, e che le stesse limitano diritti costituzionalmente rilevanti, primo fra tutti l'art. 14 Cost., si deve inevitabilmente affrontare tale questione.

Per una parte della dottrina gli elementi eventualmente acquisiti con queste modalità andrebbero incontro alla sanzione processuale della inutilizzabilità per violazione di un divieto desumibile dalla Carta fondamentale o dalla Convenzione europea[57].

"trojan"): un appello al legislatore da parte di numerosi docenti di diritto italiani, in www.penalecontemporaneo.it, 7 ottobre 2016.

[56] Come correttamente osserva P. Bronzo, *L'impiego del* trojan horse, cit., p. 350 sono proprio gli impieghi del captatatore che non hanno ricevuto «alcuna regolamentazione nel nuovo decreto legislativo si annoverano quelli più temibili: le tecniche *on line search* su tutte, che consentono un *profiling* personale ... accurato quanto mai potrebbe essere quello consentito dalle indagini tradizionali, e un'aggressione dell'intimità individuale che lambisce l'inviolabilità della psiche».

[57] In questo senso C. Conti-M. Testa, *Spionaggio informatico nell'ambito dei* social network, in *Le indagini atipiche*, cit., p. 429; F. Iovene, *Le c.d. perquisizioni* online, cit., p. 341; S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, p. 775, il quale dopo aver osservato che questa sarebbe la conclusione più lineare, mette in evidenza che l'inutilizzabilità si potrebbe costruire anche seguendo quanto stabilito dalla Corte di Giustizia UE dell'8 aprile 2014. Di fatto aderiscano alla stessa impostazione sebbene sia pur con diversi accenti A. Camon, *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove "incostituzionali"*,

Per molte delle ragioni già espresse in dottrina questa ricostruzione non appare convincente[58]. Non è questa tuttavia la sede per ripercorre compiutamente le argomentazioni più significative di questo dissenso[59]. Si può solo sottolineare che se di primo acchito la teorica della prova incostituzionale sembra essere quella in grado di fornire una più efficace tutela dei diritti inviolabili, offrendo una risposta sanzionatoria di immediata applicazione, ad un esame più attento questa certezza si dimostra ingannevole. Questa speciale forma di tutela poggerebbe di fatto sulla sensibilità dell'interpreti ed *in primis* dei giudici, ai quali verrebbe assegnato il compito di stabilire, volta per volta, l'effettiva esistenza di situazioni lesive di un diritto inviolabile.

Ma non solo. L'attribuzione di questo potere all'autorità giudiziaria non appare assolutamente in sintonia con il sistema di garanzie ideato dalla nostra Carta per tutelare i diritti inviolabili, la quale non affida certamente all'autorità giudiziaria il compito di individuare «casi e modi» delle limitazioni alle libertà individuali.

Come sottolineato da attenta dottrina quando ci si misura con il sistema di garanzie dei diritti fondamentali non è così difficile imbattersi in lacune ed antinomie: «possibili e in qualche misura inevitabili nei sistemi multilivello come sono tipicamente quelli dotati di costituzioni rigide»[60].

---

in *Cass. pen*., 1999, p. 120 ss.; L. P. Comoglio, *L'inutilizzabilità "assoluta" delle prove "incostituzionali"*, in *Riv. dir. proc*., 2011, p. 43 ss.; F. Dinacci, *L'inutilizzabilità nel processo penale*, Milano, 2008, p. 75 ss.; L. Filippi, L'home watching: *documento, prova atipica o prova incostituzionale*, in *Dir. pen. proc*., 2001, p. 9; O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont*., *Riv. Trim*., 2013, p. 8; S. Ruggieri, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni*, Milano, 2001, p. 64 ss.; G. Spangher, *"E pur si muove": dal* male captum bene retentum *alle* exclusionary rule, in *Giur. cost*., 2001, p. 2829.

58 Per un giudizio assolutamente critico sulla teoria della prova incostituzionale F. Cordero, *Tre studi sulle prove penali*, Milano, 1963, p. 153 ss. Più recentemente F. Caprioli, *Colloqui riservati e prova penale*, Milano, 2000, p. 236; N. Galantini, *Inutilizzabilità della prova e diritto vivente*, in *Riv. it. dir. e proc. pen*., 2012, p. 76 ss.

59 Tra le varie proposte formulate in dottrina per sanzionare le c.d. perquisizioni on line appare condivisibile quella secondo la quale in carenza di una disciplina normativa le stesse «a rigore dovrebbero essere ritenute addirittura giuridicamente inesistenti»: così M. Daniele, *Contrasto al terrorismo*, cit., p. 405.

60 Cfr. L. Ferraioli, Iura paria. *I fondamenti della democrazia costituzionale*, Napoli, 2017, p. 109 ss., al quale si deve anche il virgolettato che segue nel testo.

Queste manchevolezze possono essere interpretate tuttavia in un'unica maniera: «come un'indebita lacuna che è obbligatorio colmare».

Bibliografia

Aa. Vv., *Fisionomia costituzionale del processo penale*, a cura di G. Dean, Torino, Giappichelli, 2007.

Aa. Vv., *Processo penale e costituzione*, a cura di F.R. Dinacci, Milano, Giuffrè, 2011.

AMATO, Giuliano. *Individuo e autorità nella disciplina della libertà personale*, Milano, Giuffrè, 1967.

AMATO, Giuliano. Sub *artt. 13-14 Cost.*, in *Commentario della Costituzione*, a cura di G. Branca, *Rapporti civili*, Roma-Bologna, Zanichelli, 1977, p. 57.

AMORTH, Antonio. *La Costituzione italiana*, Milano, Giuffrè, 1948.

ATERNO, Stefano. Digital forensics *(investigazioni informatiche)*, in *Dig. disc. pen.*, Agg. VIII, Torino, Utet, 2014.

BALDASSARRE, Antonio. Voce *Diritti inviolabili*, in *Enc. giur. Treccani*, X, Roma, 1989.

BALDINI, Vincenzo. *"Che cosa è un diritto fondamentale". La classificazione dei diritti fondamentali. Profili storico-teorico positivi*, in www.dirittifondamentali.it, 15 giugno 2016.

BALSAMO, Antonio. *Le intercettazioni mediante* virus *informatico tra processo penale italiano e Corte europea,* in *Cass. pen.*, 2016, p. 2274.

BONO, Gaetano. *Il divieto di indagini* «ad explorandum» *include i mezzi informatici di ricerca della prova*, in *Cass. pen.*, 2013, p. 1523.

BRICOLA, Franco. *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen.*, 1967, p. 1120.

BRIGHI, Raffaella. *Funzionamento e potenzialità investigative del* malware, in *Nuove norme in tema di intercettazioni*, a cura di G. Giostra e R. Orlandi, Torino, Giappichelli, 2018, p. 211.

BRONZO, Pasquale. *Intercettazioni ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in *Nuove norme in tema di intercettazioni*, a cura di G. Giostra e R. Orlandi, Torino, Giappichelli, 2018, p. 239.

BRONZO, Pasquale. *L'impiego del* trojan horse *informatico nelle indagini penali*, in *Riv. it. scienze giur.*, 2017, p. 347.

CAIANELLO, Michele. *Il principio di proporzionalità nel procedimento penale*, in *Diritto penale contemporaneo*, *Riv. trim.*, 2014, p. 144.

CALAMANDREI, Piero, *L'avvenire dei diritti di libertà*, Giulianova, Galaad Edizioni, 2018.

CAMON, Alberto. *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen*., 1999, p. 120.

CAMON, Alberto. *Le intercettazioni nel processo penale*, Milano, Giuffrè, 1996.

CAMON, Alberto. *Cavalli di Troia in Cassazione*, in *Arch. n. proc. pen*., 2017, p. 76.

CAPONE, Arturo. *Intercettazioni e costituzione. Problemi vecchi e nuovi*, in *Cass. pen*., 2017, p. 1267.

CAPRIOLI, Francesco. *Colloqui riservati e prova penale*, Milano, Giuffrè, 2000.

CAPRIOLI, Francesco. *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. Bras. Direito Proc. Pen*., 2017, 2, p. 483.

CISTERNA, Alberto. *Spazio ed intercettazioni, una* liaison *tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite*, in *Arch. pen*., II, p. 331.

COMOGLIO, Luigi Paolo. *L'inutilizzabilità "assoluta" delle prove "incostituzionali"*, in *Riv. dir. proc*., 2011, p. 43.

CONSO, Giovanni. *Costituzione e processo penale*, Milano, Giuffrè, 1969.

CONTI, Carlotta- TESTA, Marco. *Spionaggio informatico nell'ambito dei* social network, in *Le indagini atipiche*, a cura di A. Scalfati, Torino, Giappichelli, 2014, p. 429.

CORDERO, Franco. *Tre studi sulle prove penali*, Milano, Giuffrè 1963.

DANIELE, Marcello. *Contrasto al terrorismo e captatori informatici*, in *Riv. dir. proc*., 2017, p. 403.

DANIELE, Marcello. *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. pen e giust*., 5, 2018, p. 831.

DE FLAMMINEIS, Siro. *Le intercettazioni telematiche*, in *Dir. pen. proc*., 2013, p. 989.

DI PAOLO, Gabriella. *Prova informatica (dir. proc. pen.)*, in *Enc. dir*. annali, VI, Milano, Giuffrè, 2016, p. 73.

DINACCI, Filippo. *L'inutilizzabilità nel processo penale*, Milano, Giuffrè, 2008, p. 75.

ELIA, Leopoldo. *Le misure di prevenzione fra l'art. 13 e l'art. 25 della Costituzione*, in *Giur. cost*., 1964, p. 940.

ESPOSITO, Roberto. *Politica e negazione. Per una filosofia affermativa*, Torino, Einaudi, 2018.

FELICIONI, Paola. *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. giust*., 2016, fasc. 5, p. 21.

FERRAJOLI, Luigi. Iuria paria. *I fondamenti della democrazia costituzionale*. Napoli, Editoriale Scientifica, 2017.

FILIPPI, Leonardo. L'home watching: *documento, prova atipica o prova incostituzionale*, in *Dir. pen. proc.*, 2001, p. 9.

FILIPPI, Leonardo. *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico)*, in *Arch. pen.*, 2016, II, p. 348.

FONTI, Rossella. *La tutela costituzionale delle libertà individuali*, in *Fisionomia costituzionale del processo penale*, a cura di G. Dean, Torino, Giappichelli, 2007, p. 11.

FOUCAULT, Michel. *Nascita della biopolitica. Corso al College de France* (1978/1979), trad. it., Milano, Feltrinelli 2005.

GAITO, Alfredo-FURFARO, Sandro. *Le nuove intercettazioni ambulanti: tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza della collettività*, in *Arch. pen.*, 2016, II, p. 309.

GALANTINI, Novella. *Inutilizzabilità della prova e diritto vivente*, in *Riv. it. dir. e proc. pen.*, 2012, p. 76.

GALLUCCIO, Alessandra. *Profili generali sugli artt. 8-11*, in *Corte di Strasburgo e giustizia penale*, a cura di G. Ubertis e F. Viganò, Torino, Giappichelli, 2016, p. 257-261.

GIORDANO, Luca. *Dopo le sezioni unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Diritto penale contemporaneo*, 20 marzo 20.

GRIFFO, Mario. *Una proposta costituzionale per arginare lo strapotere del captatore*, in *Diritto penale contemporaneo*, 2, 2018, p. 24.

GROSSI, Pierfrancesco. *Introduzione ad uno studio sui diritti inviolabili nella Costituzione italiana*, Padova, Cedam, 1972.

IOVENE, Federica. *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze dell'accertamento penale*, in *Diritto penale contemporaneo*, 2014, p. 336.

LASAGNI, Giulia. *L'uso dei captatori informatici (*trojans*) nelle intercettazioni tra presenti*, in Diritto penale contemporaneo, 7 ottobre 2016, p. 15.

ILLUMINATI, Giulio. *La tutela della segretezza delle comunicazioni tra vecchio e nuovo codice*, in *Processo penale e valori costituzionali nell'insegnamento di Vittorio Grevi*, Padova, Cedam, 2013, p. 106.

LUCIANI, Massimo. *La produzione economica privata nel sistema costituzionale*, Padova, Cedam, 1983.

LUCIANI, Massimo. *Positività e meta positività e parapositività dei diritti fondamentali*, in *Scritti in onore di L. Carlassare, Il diritto costituzionale come regola e limite al potere*, Napoli, Jovene, 2009, II, p. 1067.

LUPARIA, Luca. Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, dir. G. Spangher, *Modelli differenziati di accertamento*, a cura di G. Garuti, t. I, Torino, Utet, 2011, p. 396 ss.;

MANGIAMELI, Stelio. *Il contributo dell'esperienza costituzionale italiana alla dommatica europea della tutela dei diritti fondamentali*, in *Corte costituzionale e processo costituzionale*, a cura di A. Pace, Milano, Giuffrè, 2006, p. 471.

MARCOLINI, Stefano. *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015.

MAZZA, Oliviero. *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Diritto penale contemporaneo*, *Riv. Trim.*, 2013, p. 8.

MORTATI, Costantino. *Istituzioni di diritto pubblico*, II, 8° ed., Padova, Cedam, 1969.

NICOLICCHIA, Fabio. *I limiti fissati dalla Corte costituzionale tedesca agli strumenti di controllo tecnologico occulto: spunti per una trasposizione nell'ordinamento italiano*, in www.archiviopenale.it, 2017.

NICOLICCHIA, Fabio. *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in Diritto penale contemporaneo, 8 gennaio 2018.

NIETZCHE, Friedrich. *Crepuscolo degli idoli*, in *Opere*, a cura di G. Colli e M. Montinari, Vol. VI, t. III, Milano, Adelphi, 1991, p. 113.

ORLANDI, Renzo. *La riforma del processo penale fra correzioni strutturali e tutela progressiva dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, p. 1133.

ORLANDI, Renzo. *Osservazioni sul documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in www.archiviopenale.it, 25 luglio 2016.

PARLATO, Lucia. *Problemi insoluti: le perquisizioni* on-line, in *Nuove norme in tema di intercettazioni*, a cura di G. Giostra e R. Orlandi, Torino, Giappichelli, 2018, p. 295.

PICOTTI, Lorenzo. *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. pen.*, 2016, II, p. 354.

PINELLI, Cesare. *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "*virus *di Stato"*, in *Diritto penale contemporaneo*, 2017, p. 82.

RUGGIERI, Stefano. *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni*, Milano, Giuffrè, 2001.

SIGNORATO, Silvia. *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, Giappichelli, 2018.

SIGNORATO, Silvia. *Modalità procedimentali dell'intercettazione tramite captatore informatico*, in *Nuove norme in tema di intercettazioni*, a cura di G. Giostra e R. Orlandi, Torino, Giappichelli, 2018, p. 263.

SILVESTRI, Gaetano. *L'individuazione dei diritti della persona*, in *Diritto penale contemporaneo*, 27 ottobre 2018.

SPANGHER, Giorgio. *"E pur si muove": dal* male captum bene retentum *alle* exclusionary rule, in *Giur. cost*., 2001, p. 2829.

TESTAGUZZA, Alessandra. *I sistemi di controllo remoto: fra normativa e prassi*, in *Diritto penale e proc*esso, 2014, p. 759.

TORRE, Marco. *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Diritto penale e processo*, 2015, p. 1168-1170.

TROGU, Mauro. *Sorveglianza e "perquisizioni" online su materiale informatico*, in *Le indagini atipiche*, a cura di A. Scalfati, Torino, 2014, p. 444

VENEGONI, Andrea-GIORDANO, Luca. *La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazione da remoto a mezzo di strumenti informatici*, in *Diritto penale contemporaneo*, 8 maggio 2016.

Informações adicionais e declarações dos autores (*integridade científica*)

Declaração de conflito de interesses (conflict of interest declaration): o autor confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores.

Declaração de ineditismo e originalidade (declaration of originality): o autor assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 10/7/2019
- Controle preliminar e verificação de plagio: 23/8/2019
- Avaliação 1: 30/9/2019
- Avaliação 2: 03/10/2019
- Decisão editorial preliminar: 03/10/2019
- Retorno rodada de correções: 05/10/2019
- Decisão editorial final: 08/10/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editoras-associadas: 2 (CC e BC)
- Revisores: 2

COMO CITAR ESTE ARTIGO:

ALONZI, Fabio. L'escalation dei mezzi di intrusione nella sfera privata: ripartire dalla Costituzione. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1421-1448, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.259

Compatibilizando o uso de tecnologia em investigações com direitos fundamentais: o caso das interceptações ambientais

Reconciling the use of technology in investigations with fundamental rights: the case of monitoring of public and private spaces

Jacqueline de Souza Abreu[1]

Faculdade de Direito da Universidade de São Paulo – São Paulo/SP

jacqueline.abreu@usp.br

http://lattes.cnpq.br/6550261352169681

https://orcid.org/0000-0003-0450-4102

Gianluca Martins Smanio[2]

Faculdade de Direito da Universidade de São Paulo – São Paulo/SP

gianluca.smanio@usp.br

http://lattes.cnpq.br/2870717531871935

https://orcid.org/0000-0002-9219-1654

Resumo: Avanços tecnológicos oferecem ferramentas para autoridades de investigação que levantam questionamentos à luz da proteção a direitos fundamentais. Este artigo estuda o processo de compatibilização pelo qual uma dessas ferramentas tem passado: as interceptações ambientais de sinais ópticos, acústicos e eletromagnéticos. Ainda hoje, a medida possui breve regulamentação jurídica no ordenamento brasileiro, mencionada no artigo 3º, II, da Lei n.º 12.850/2013. Como meio de obtenção de prova caracterizado pelo caráter sigiloso e invasivo ao lar, à intimidade,

[1] Doutoranda em Direito na Universidade de São Paulo, Departamento de Filosofia e Teoria Geral do Direito. Mestra em Direito pela University of California, Berkeley (EUA) e pela Ludwig-Maximilians-Universität München (Alemanha). Advogada em São Paulo - SP.

[2] Mestrando em Direito na Universidade de São Paulo, Departamento de Direito Processual, subárea de Processo Penal. Advogado em São Paulo - SP.

às comunicações e mesmo à autodeterminação informacional, é fundamental que seja dotado de regramento pormenorizado em lei a fim de evitar arbítrios incompatíveis com direitos fundamentais. Com o objetivo de contribuir para esse processo, este artigo reconstrói o processo de incorporação dessa medida investigativa ao direito brasileiro. A seguir, e a partir da lição do Tribunal Europeu de Direitos Humanos, discute-se a regulamentação da medida, engajando-se criticamente com o recente Projeto de Lei Anticrime.

Palavras-chave: interceptação ambiental; escuta ambiental; meio de obtenção de prova; direitos fundamentais; sigilo das comunicações.

Abstract: *Technological advances offer tools to law enforcement authorities that must be reconciled with the protection of fundamental rights. This article discusses the compatibilization process of one of these tools: the case of interception of optical, acoustic and electromagnetic signals in public and private spaces. This tool is briefly mentioned in Brazilian law, present only in the article 3, II, of the Law n.º 12.850/2013. As an evidence gathering method, known for its secrecy and invasiveness, it is of the most importance to restrain its use with more detailed laws that reconcile the tool with fundamental rights. In order to contribute to this process, this article reviews how this monitoring tool has been incorporated into Brazilian law and discussed in scholarship. Next, in light of the lessons of the European Court of Human Rights, a provision found in the recent "Anti-crime" bill that would further incorporate the tool in Brazilian law is critically discussed.*

Keywords: *interception of optical, acoustic and electromagnetic signals; surveillance; means to gather and obtain evidence; fundamental rights; secrecy of communications.*

INTRODUÇÃO

A realização de interceptações ambientais levanta questionamentos jurídicos desde que gravadores foram desenvolvidos e se apresentaram como possível ferramenta de investigação para obtenção de provas. Nelas, há captação de conversa mantida entre duas ou mais pessoas *presentes*, fora do telefone ou da internet, em algum recinto, privado ou público. São, portanto, um exemplo clássico de como uma ferramenta tecnológica influencia a prática do direito processual penal. Como o avanço tecnológico não para, expandem-se também as possibilidades e capacidades da medida: pode ser e é utilizada não mais apenas para se referir à captura do fluxo de *comunicação* de voz entre presentes (sinais acústicos), mas também de imagens (sinais ópticos) e sinais eletromagnéticos de forma mais abrangente, capturados de um certo ambiente em tempo real.

O presente trabalho versa sobre uma questão permanente – e cada vez mais urgente, diante das crescentes potencialidades ofertadas pelo avanço tecnológico - sobre *interceptações ambientais*: como deve ser ajustado nosso regime jurídico para que discipline essa medida investigativa de modo compatível com direitos fundamentais? Primeiro, é analisado o regime jurídico hoje existente no Brasil aplicável a essa medida, tanto da perspectiva da constitucionalidade desse meio de investigação quanto de sua legalidade e tendo em vista tanto a doutrina quanto a jurisprudência. A seguir, o artigo apresenta a experiência do Tribunal Europeu de Direitos Humanos com o tema para destacar os principais aspectos levados em conta pelo tribunal ao analisar a compatibilidade desse tipo de medida restritiva com direitos humanos. Por fim, à luz das observações feitas nos tópicos anteriores, analisamos o Projeto de Lei Anticrime (Projeto de Lei n.º 882/2019) do atual Ministério da Justiça, que propõe a inserção do meio de obtenção de prova no diploma legal da Lei das Organizações Criminosas (Lei n.º 12.850/2013).

Para qualquer pessoa preocupada em estudar o impacto da tecnologia no processo penal, a interceptação ambiental é um bom estudo de caso. Como esperamos mostrar ao longo do trabalho, esse meio de investigação foi incorporado ao ordenamento brasileiro sem maiores preocupações regulatórias - específicas do tipo de tecnologia em questão e com o contexto de sua aplicação. Por causa disso, a validade de provas

produzidas por essa medida é ainda hoje questionada em diversos aspectos. Sem dúvidas, esse é um processo pelo qual passam e passarão diversas outras ferramentas tecnológicas que hoje se colocam à disposição de autoridades de investigação. As perguntas aqui colocadas e as observações extraídas podem ser, portanto, levadas para diversos outros casos.

1. REGIME JURÍDICO APLICÁVEL A INTERCEPTAÇÕES AMBIENTAIS

1.1. Breve Histórico

A noção de "interceptação ambiental" se inseriu na prática jurídica fundamentalmente com o propósito de qualificar um certo tipo de atividade de obter provas no âmbito de processo penal. Por isso se diz que sua natureza jurídica é a de *meio de obtenção ou de pesquisa de provas*, o que é feito em geral como providência cautelar como ato de investigação em fase pré-processual.[3] Pela própria natureza dessa medida, ela é incompatível com o exercício do contraditório pleno, já que não haveria, via de regra, condições de atingir seu objetivo se fosse implementada com o conhecimento da pessoa ou das pessoas que se pretende monitorar.

O primeiro marco legal que trouxe a figura da interceptação ambiental ao ordenamento jurídico brasileiro foi a Lei n.º 9.034/1995, a antiga lei que regulava "meios de prova e procedimentos investigatórios que versem sobre ilícitos decorrentes de ações praticadas por quadrilha ou bando ou organizações ou associações criminosas de qualquer tipo" (art. 1º). Isso aconteceu quando, em 11 de abril de 2001, foi inserido pela Lei n.º 10.217/2001 o inciso IV no artigo 2º, prevendo "a captação e a interceptação ambiental de sinais eletromagnéticos, óticos ou acústicos, e o seu registro e análise, mediante circunstanciada autorização judicial".

---

[3] GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flavio Luiz; MORAES, Maurício Zanoide (org.). *Estudos em homenagem à professora Ada Pellegrini Grinover*. São Paulo: DPJ, 2005. p. 303-318. p. 309; SIDI, Ricardo. *A interceptação das comunicações telemáticas no processo penal*. Belo Horizonte: D'Plácido, 2016. p. 60-62.

No mais, na época, a doutrina tinha entendimento no sentido de aplicação, de forma análoga, do procedimento da Lei n.º 9.296/1996, a Lei das Interceptações Telefônicas, ela mesma já alvo de severas críticas[4]. No julgamento do Inquérito 2.424, o Supremo Tribunal Federal considerou que a ausência de maior detalhamento do procedimento em lei não era razão de nulidade desse meio de prova.[5]

Em 2013, a Lei n.º 9.034/1995 foi ab-rogada pela Lei n.º 12.850/2013, que trouxe a nova regulamentação dos procedimentos probatórios referentes a organizações criminosas. Nela se admite que "em qualquer fase da persecução penal" será permitida a "captação ambiental de sinais eletromagnéticos, ópticos ou acústicos" como meio de obtenção de prova (art. 3º, inciso II). Considerando a legislação em que foi inserida, temos uma restrição do seu âmbito de aplicação apenas aos casos em que se constate a presença de organização criminosa[6]. No mais,

---

[4] C.f.: SILVA, Eduardo Araujo da. *Crime Organizado*: procedimento probatório. 2ª ed. São Paulo: Atlas, 2009. e DEZEM, Guilherme Madeira. *Da prova penal:* tipo processual, provas típicas e atípicas: (atualizado de acordo com as Leis 11.689/08, 11.690/08 e 11.719/08). Campinas: Millenium, 2008. p. 299-308. Em sentido contrário: MALAN, Diogo. Gravações Ambientais Domiciliares no Processo Penal. In: LIMA, José Corrêa de; CASARA, Rubens R. R. (coord.). *Temas para uma perspectiva crítica do Direito:* homenagem ao Professor Geraldo Prado. Rio de Janeiro: Lumen Juris, 2010. p. 350 e p. 355.

[5] Veja-se trecho da ementa da decisão: "PROVA. Criminal. Escuta ambiental. Captação e interceptação de sinais eletromagnéticos, óticos ou acústicos. Meio probatório legalmente admitido. Fatos que configurariam crimes praticados por quadrilha ou bando ou organização criminosa. Autorização judicial circunstanciada. Previsão normativa expressa do procedimento. Preliminar repelida. Inteligência dos arts. 1º e 2º, IV, da Lei nº 9.034/95, com a redação da Lei nº 10.217/95. Para fins de persecução criminal de ilícitos praticados por quadrilha, bando, organização ou associação criminosa de qualquer tipo, são permitidos a captação e a interceptação de sinais eletromagnéticos, óticos e acústicos, bem como seu registro e análise, mediante circunstanciada autorização judicial." SUPREMO TRIBUNAL FEDERAL. Inq. 2.424. Min Rel. Cezar Peluso. Data de julgamento 26 de março de 2009. Ver também "Informativo 529" do STF.

[6] Eduardo Araújo da Silva defende que o legislador, ao estabelecer o meio de obtenção de prova na Lei n.º 12.850/13, orientou-se pelo princípio da proporcionalidade, uma vez que a lei trata exatamente da apuração de crimes praticados por organização criminosa (SILVA, Eduardo Araújo da. *Organizações Criminosas:* Aspectos Penais e Processuais da Lei n.º 12.850/2013. 2ª ed.

ao contrário do que ocorre para outros meios ali previstos, como a colaboração premiada, a ação controlada, e a infiltração de agentes, a lei não dedicou nenhuma seção para elencar os parâmetros que devem nortear a execução dessa medida. Comparada à redação original da lei anterior, nota-se que se omitiu inclusive a expressa referência à necessidade de "circunstanciada autorização judicial", dando abertura para que a medida seja empregada sem decisão judicial prévia.

1.2. A tipicidade e a atipicidade dos meios de obtenção de prova

Essa previsão em si não encerra discussões sobre a juridicidade dessa medida - e, na verdade, essa opção legislativa repercute fundamentalmente na análise sobre a tipicidade das interceptações ambientais. Afinal, no Processo Penal Brasileiro, por mais que não vigore um sistema de taxatividade da prova penal, é importante que haja previsão legal desta e do procedimento pelo qual será colhida e inserida nos autos. Isso permite aos sujeitos processuais maior segurança, uma vez que podem tomar conhecimento, de forma precisa, dos requisitos necessários para a produção probatória, evitando eventuais nulidades procedimentais, além de deixar claro os direitos de cada um dos sujeitos, em especial as garantias processuais[7].

Arantes Filho, após análise do desenvolvimento da discussão sobre tipicidade probatória nas doutrinas italiana e brasileira, traz que, para uma prova ser *típica*, é necessário que seja admissível, englobando a nominação e seus requisitos e o rito probatório, para assim formar o conjunto da disciplina legal do instituto.[8] Logo, uma prova atípica é

São Paulo: Atlas, 2017.). Everton Luiz Zanella coloca que é meio de obtenção de prova "destinado a combater organizações criminosas" (ZANELLA, Everton Luiz. *Infiltração de agentes no combate ao crime organizado*: análise do mecanismo probatório sob o enfoque da eficiência e o garantismo. Curitiba: Juruá, 2016. p. 162.

[7] DEZEM, Guilherme Madeira. *Curso de Processo Penal*. São Paulo: Revista dos Tribunais, 2015. p. 447.

[8] ARANTES FILHO, Marcio Geraldo Britto. *A interceptação de comunicação entre pessoas presentes*. Brasília: Gazeta Jurídica, 2013. p. 44-45.

aquela não catalogada ou regulada em lei[9]. Segundo a teoria ampliativa da atipicidade probatória, pode-se ter uma prova atípica tanto nos casos em que há previsão legal, mas não há regulamentação de seu procedimento probatório, quanto nos casos em que nem o meio de prova, nem seu procedimento tenham previsão legal[10].

Nesse contexto, considera-se que, quanto à sua admissibilidade, interceptações ambientais são um meio de prova nominado, disposto no art. 3º, II, da Lei n.º 12.850/2013. No entanto, não há presença de requisitos, além da permissão de seu deferimento caso se constate presença de organização criminosa (art. 1º, *caput*, e definição do conceito de organização criminosa no §1º), pressuposto simples frente ao seu caráter sigiloso e restritivo de garantias constitucionais, como se verá melhor à frente. Quanto ao rito probatório, não há lei que regulamente especificamente a interceptação ambiental. Temos, nesse sentido, o que a doutrina denomina de "prova nominada", por haver *nomen juris* previsto em lei, mas atípica, uma vez que não possui procedimento próprio[11].

A doutrina aponta que o motivo da omissão legislativa é possível de ser encontrado na exposição de motivos do projeto que originou tal lei: "o legislador entendeu *desnecessária* a criação de procedimento probatório autônomo para a captação ambiental de sinais eletromagnéticos, óticos ou acústicos, por entender que lhe é aplicável, *por analogia,*

---

[9] GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flavio Luiz; MORAES, Maurício Zanoide (org.). *Estudos em homenagem à professora Ada Pellegrini Grinover*. São Paulo: DPJ, p. 303-318, 2005. p. 314.

[10] Segundo Dezem, para a posição ampliativa, "*tem-se que uma prova é atípica em duas situações:(1) quando ela seja prevista no ordenamento, mas não o seja seu procedimento probatório; (2) quando nem ela nem seu procedimento probatório sejam previstos em lei*". (DEZEM, Guilherme Madeira. *Curso de Processo Penal*. São Paulo: Revista dos Tribunais, 2015. p. 445).

[11] DEZEM, Guilherme Madeira. *Da prova penal:* tipo processual, provas típicas e atípicas: (atualizado de acordo com as Leis 11.689/08, 11.690/08 e 11.719/08). Campinas: Millenium, 2008. p. 156-157. Arantes Filho delimitou a prova atípica aos seguintes casos: "*a prevista em lei, sem o respectivo procedimento probatório (próprio ou por remissão), a referida nominalmente em lei e a não referida em lei.*". Já a nominada "*é a prevista em lei, com ou sem delimitação de procedimento probatório.*" (ARANTES FILHO, Marcio Geraldo Britto. *A interceptação de comunicação entre pessoas presentes*. Brasília: Gazeta Jurídica, 2013. p. 45).

o rito da interceptação de comunicações telefônicas e telemáticas (Lei 9.296/1996)".[12] O problema é que, assim como no passado, a aplicação analógica de tal lei para interceptações ambientais não é pacífica na doutrina, apesar de a equiparação ser frequente na jurisprudência; voltaremos a este ponto mais a frente.

Por ora, frente a esse cenário, cabe analisar dogmaticamente se e em que condições interceptações ambientais podem ser utilizadas como meio de prova, segundo o paradigma constitucional. Para tanto, seguiremos o cotejo analítico avançado por Dezem. Em sua obra, ele estipula duas condições, de maneira cumulativa, para que a *atipicidade* seja lícita e o meio de investigação de prova possa ser utilizado: em primeiro lugar, *não pode haver violação a qualquer direito fundamental individual ao longo de sua produção*; em segundo lugar, *deve haver meio de prova típico*, ou seja, admissível e com procedimento probatório definido em lei, *que possa ser aplicado analogicamente*.[13] Nas subseções que seguem, discutiremos esses pontos. Ao ingressarmos nessa discussão, é importante ter em mente que provas obtidas em violação a normas constitucionais, substantivas ou processuais, são inadmissíveis.[14]

1.3. Constitucionalidade: Interceptações Ambientais e Direitos Fundamentais

Uma preocupação transversal a todos os tipos de interceptação é a questão da constitucionalidade dessa medida, conquanto afeta direitos fundamentais. Nessa seção, cuidamos de analisar os direitos constitucionais implicados na execução de medidas de interceptação ambiental a partir

---

[12] MALAN, Diogo. Da Captação Ambiental de sinais eletromagnéticos, óticos, ou acústicos e os limites relativos à privacidade. AMBOS, Kai; ROMERO, Eneas (coord.). *Crime Organizado:* Análise da Lei 12. 850/2013. São Paulo: Marcial Pons, 2017. p. 51-81. p. 57.

[13] DEZEM, Guilherme Madeira. *Da prova penal:* tipo processual, provas típicas e atípicas: (atualizado de acordo com as Leis 11.689/08, 11.690/08 e 11.719/08). Campinas: Millenium, 2008. p. 275 e ss.

[14] GOMES FILHO, Antonio Magalhães; BADARÓ, Gustavo. Prova e sucedâneos da prova no processo penal brasileiro. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 15, n. 65, p. 175-208, mar./abr., 2007. p. 198.

do rol de direitos fundamentais encontrados na Constituição Federal brasileira de 1988: o direito à privacidade[15], o direito à inviolabilidade do domicílio[16] e o direito ao sigilo das comunicações.[17]

1.3.1. Interceptações ambientais e a proteção da vida privada

Um primeiro direito constitucional que pode ser afetado por interceptações ambientais é aquele previsto no inciso X do art. 5º da Constituição Federal, que protege a intimidade e a vida privada. Trata-se fundamentalmente de proteção ao conjunto de informações sobre as quais o indivíduo deve ter poder de controle sobre guardar em sigilo para si ou comunicar, com quem, onde e nas condições que quiser.[18] É por isso que sequer se questiona a legalidade de interceptações quando há *notificação e consentimento* daqueles que estão sendo gravados. Neste caso, os atores afetados dispõem sobre seu direito, concordando com o registro de informações por eles comunicadas. Em sendo assim, não há que se falar, a princípio, em interferência nesse direito mesmo quando as comunicações registradas dizem respeito a imagens e conversas que possam ter conteúdo íntimo, desde que a coleta e o uso dessas informações permaneçam vinculados aos fins a que foram coletados e com os quais os *interceptados* concordaram.

---

15 "*Art. 5º, X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação*."

16 "*Art. 5º, XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial.*"

17 "*Art. 5º, XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal*". Ver ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *Vigilância sobre as comunicações no Brasil:* interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. p. 21.

18 SILVA, José Afonso. *Curso de Direito Constitucional*. 32ª ed. São Paulo: Malheiros, 2009. p. 206.

Na ausência de notificação e de consentimento, as interceptações interferem nesses direitos à intimidade e vida privada, especialmente quando utilizadas para obter informações que os interlocutores afetados buscam manter sobre controle quanto à sua publicidade. Quanto mais sensíveis as informações obtidas, maior a invasão à privacidade concretizada pela interceptação ambiental.

1.3.2. Interceptações ambientais e a proteção de ambientes públicos e privados

Quando a interceptação ambiental ocorre em local privado, como um domicílio, seja ele familiar ou profissional, os interesses relacionados à inviolabilidade do domicílio, protegidos no art. 5º, XI, da Constituição Federal, estão especialmente presentes. Essa característica faz com que o grau da invasão decorrente de uma interceptação de ambiente privado seja especialmente maior por acarretar intromissão em relações domésticas, familiares, de esfera privada, já que se entende que são nesses espaços que se realizam condutas que servem para o desenvolvimento individual.[19] O mesmo acontece em certos domicílios profissionais e, principalmente, naqueles resguardados pela proteção de sigilo profissional.[20]

Mais difícil é o caso em que a interceptação ambiental ocorre em ambiente público: algum direito é afetado? Nesse caso, apesar de ainda incipiente no Brasil, principalmente em razão da falta de previsão expressa no texto da constituição e da cultura jurídica ainda pouco sensível ao tema, o interesse de "privacidade" afetado traduz-se, pelo que se vê no direito comparado, na *autodeterminação informativa,* termo utilizado para se referir ao direito com o qual se pretende garantir controle de indivíduos sobre produção e uso de dados que lhe digam respeito, concepção que foi desenvolvida doutrinária e jurisprudencialmente frente

---

[19] Ver SILVA, José Afonso. *Curso de Direito Constitucional*. 32ª Ed. São Paulo: Malheiros, 2009. p. 207; ROXIN, Claus. *La prohibición de autoincriminación y de las escuchas domiciliarias*. Buenos Aires: Hammurabi, 2008. p. 91.

[20] SILVA, José Afonso. *Curso de Direito Constitucional*. 32ª Ed. São Paulo: Malheiros, 2009. p. 207-208.

aos avanço da tecnologia e dos riscos decorrentes da coleta massiva e do uso inesperado de dados pessoais.[21]

A noção relevante para a matéria de interceptações ambientais é que, mesmo que ao ingressar no domínio público se abra mão do domínio exclusivo de algumas informações pessoais daqueles com quem se compartilha o espaço público, quando um meio permanente *registra* o que é feito em público, algo de diferente acontece. Isso porque, sem o uso de tecnologias de gravação, as informações que compartilhamos em público são retidas apenas temporariamente na memória de um número reduzido de pessoas. Quando há o registro permanente por meio de gravação de áudio ou vídeo, *aumentam-se* os riscos aos quais se está exposto: desde exposição a um número inesperado de pessoas até à agregação de dados e extração de análises de comportamento que podem ser usados contra o próprio indivíduo, em estratégias comerciais ou mesmo políticas.[22] Por essa razão, mesmo nesse caso há ou pelo menos pode haver restrição de interesse relevante, se a autodeterminação informativa for interpretada como mais uma faceta do direito de personalidade.

1.3.3. Interceptações ambientais e a proteção ao sigilo das comunicações

Claramente, pela linguagem do inciso XII do art. 5º da Constituição Federal, as interceptações de comunicações *telefônicas* são medidas que o constituinte admitiu como, pelo menos em princípio, constitucionais, desde que observados certos parâmetros previstos em lei.[23] O que dizer

---

[21] Ver DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006. p. 204; MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*. São Paulo: Saraiva, 2014. p. 32.

[22] Ver MOORE, Adam D. *Privacy Rights:* Moral and Legal Foundations. Pennsylvania: Penn State University, 2010. p. 90-91.

[23] Com um atraso de quase oito anos, a lei que regulamentou a exceção ali prevista para interceptações telefônicas foi aprovada e assim foram criados parâmetros para utilização desse meio de obtenção de prova. A Lei 9.296 de 1996, no entanto, também 'inovou' de outras formas e logo trouxe questionamentos sobre sua constitucionalidade: ela estendeu o seu âmbito de aplicação não só a interceptação do fluxo de comunicações telefônicas, mas também ao fluxo de "comunicações em sistemas de informática e telemática" (art. 1, parágrafo único), isto é, a comunicações *eletrônicas*. Diante disso, a constitucionalidade

das interceptações ambientais? Seriam as interceptações ambientais conciliáveis com o art. 5º, inciso XII?

Nesse contexto, vale lembrar que Ferraz Júnior defendia que as interceptações telefônicas eram as únicas que a Constituição havia admitido porque comunicações telefônicas não se perenizam em meio algum.[24] Nessa mesma linha, Badaró endossa o entendimento de que comunicações eletrônicas de navegação na internet, quando não se 'registram' em nenhum documento, também poderiam ser interceptadas por esse mesmo motivo.[25] Se é essa a racionalidade, também é possível dizer que comunicações ocorridas entre presentes, em recinto público ou privado, não se perenizam, de modo que seria ainda necessário e autorizado pela constituição garantir a possibilidade de haver *interceptação ambiental*.

Sobre essa questão, é importante notar que não é imediatamente evidente que questões relacionadas ao inciso XII do art. 5 da Constituição Federal podem ser suscitadas. Isso porque interceptações ambientais afetam comunicações *entre presentes* – não ocorridas de forma mediada.

---

de tal dispositivo foi contestada com base no entendimento baseado no texto literal do inciso XII do art. 5 de que só o fluxo de comunicações *telefônicas* poderia ser restringido para fins de persecução penal. SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade n. 1488-9/DF, Min. Néri da Silveira, julg. em 07.11.1999. Entretanto, por ter julgado ilegítima a parte proponente da ação (Associação Nacional dos Delegados de Polícia), foi negado prosseguimento ao caso; nova ação de mesmo escopo (ADI 4.112/DF) aguarda julgamento desde 2008. Atualmente, o Marco Civil da Internet (Lei 12.965 de 2014), em seu art. 7º, inciso II também prevê a possibilidade de interceptação do fluxo de comunicações pela Internet, mediante ordem judicial, "na forma da lei" (no que se vê uma referência à Lei 9.296/96). O Congresso Nacional, portanto, previu já em pelo menos dois regramentos a possibilidade de *interceptação telemática*, que também já é prática investigativa corriqueira há muitos anos. Apesar da inércia do STF sobre essa, o próprio tribunal já admitiu tacitamente a constitucionalidade dessa medida ao julgar recursos criminais em controle concreto de constitucionalidade.

[24] FERRAZ JR., Tercio Sampaio. Sigilo de Dados: o direito à privacidade e os limites da função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo,* São Paulo, v. 88, p. 439-459, 1993.

[25] BADARÓ, Gustavo. Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia. In: LIMA, José Corrêa de; CASARA, R. R. Rubens. (coord.). *Temas para uma perspectiva crítica do direito:* homenagem ao Professor Geraldo Prado. Rio de Janeiro: Lumen Juris, 2010. p. 483-499

Isso é relevante porque o sigilo ali garantido, textualmente, relaciona-se ao fluxo de informações comunicadas e transmitidas pelos meios lá citados, isto é, as correspondências, mensagens telegráficas, dados e telefonemas, meios típicos de comunicação entre *ausentes*. Apenas se o dispositivo for interpretado tendo em vista o valor que busca proteger – isto é – um direito de limitar os destinatários de uma comunicação, não importa a forma que tome, em detrimento da literalidade textual, é que se pode dizer que esse direito é implicado por interceptações ambientais. Cabe ressaltar, neste ponto, que a posição adotada depende da *teoria da interpretação* adotada pelo intérprete que, como visto, pode rejeitar ou aceitar a proposição de que o direito ao sigilo previsto no inciso XII está em jogo.

1.3.4. Análise crítica do impacto em direitos fundamentais

O objetivo dessa subseção foi mostrar que interceptações ambientais impactam diversos direitos fundamentais previstos na Constituição Federal. Na linha do raciocínio de Dezem, citado acima, para quem a atipicidade de um meio de obtenção de prova é lícita apenas se não violar direitos fundamentais, temos de concluir que essa condição não foi satisfeita. Por restringirem direitos fundamentais, as interceptações ambientais necessariamente precisariam ser típicas, rigorosamente regulamentadas em lei, além de sujeitas ao crivo judicial.

Esse não é o único paradigma que justifica tal conclusão. Dentro do modelo de avaliação de constitucionalidade de medidas restritivas a direitos fundamentais popularizado por Alexy, o fato de que uma medida estatal (aqui, um meio de investigação) interfere em direitos fundamentais faz com que o ônus na justificação dessa medida aumente. Requisito básico para isso é a atenção ao princípio da legalidade - a necessidade de que a medida seja não só prevista, mas procedimentalizada em lei, de forma a incluir salvaguardas que garantam a proporcionalidade dessa medida. Só assim é que interceptações ambientais poderiam ser fundamentadas como admissíveis em um Estado constitucional de Direito.[26] Isso pode ser atestado em decisão do Tribunal Federal

[26] ALEXY, Robert. *Teoria dos Direitos Fundamentais*. 2ª ed. São Paulo: Malheiros, 2015; ALEXY, Robert. Constitutional Rights and Proportionality.

Constitucional da Alemanha, que já se debruçou sobre o tema e chegou a declarar inconstitucional lei que previa interceptação ambiental em domicílios, mas não continha salvaguardas suficientes para resguardar a proporcionalidade dessa medida.[27]

Em que pese isso, a realidade jurisprudencial brasileira, como já acenado, é outra. No Inquérito 2.424, decidido em 2010 pelo Supremo Tribunal Federal, considerou-se que o ingresso da autoridade policial em domicílio profissional (no caso, escritório de advocacia), no período noturno para instalação de equipamento de captação, não torna nula a prova assim obtida quando a medida tiver sido autorizada por decisão judicial baseada em suspeita grave da prática de crime. Segundo a Corte, essa situação não implicaria violação da Constituição pois, no caso, o próprio advogado é suspeito da prática de crime, sobretudo concebido e consumado no âmbito desse local de trabalho. Isso significa, em outras palavras, que o STF considerou suficiente o modelo do atual regime legal em vigor - que nomeia esse meio de investigação, sem regulamentá-lo. E isso mesmo em um caso com o nível de sensibilidade maior, por envolver a questão sobre a extensão do sigilo profissional de advogados.

Como se pode notar da decisão, entretanto, o STF colocou certas balizas. A inviolabilidade do domicílio só é afastada quando há legítima suspeita de envolvimento em atividade ilícita, o que deve ser avaliado por um magistrado. A nosso ver, a melhor maneira de garantir que isso não dê lugar a abusos e arbitrariedades seria pela regulamentação detalhada em lei, que justamente serviria para nortear a atuação de controle judicial nesse sentido e elencaria outros requisitos e métodos que garantissem a conciliação com todo o sistema constitucional brasileiro, principalmente seus princípios e garantias fundamentais. Considerando essa preocupação, vale analisar a possibilidade de aplicação analógica da Lei n.º 9.296/1996.

Revus (Online), v. 22, p. 51-65, 2014. Disponível em: <http://revus.revues.org/2783>. Acesso em: 01. set. 2019. https://doi.org/10.4000/revus.2783

[27] BVerfGE 109, 279-391. Decisão de 3 de março de 2004. Disponível em: <http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html>. Acesso em 26 de maio de 2018.

1.4. Legalidade: Interceptações Ambientais e Aplicação Analógica da Lei n.º 9.296/1996

A seção anterior apresentou como interceptações ambientais afetam direitos fundamentais. Seguindo o teste proposto por Dezem para avaliar se um meio de prova atípico pode ser utilizado, outro aspecto a se analisar é se a Lei das Interceptações Telefônicas poderia ser aplicada analogicamente para interceptações ambientais. Parte da doutrina responde negativamente, enquanto outra parte determina ser imperioso o uso análogo, no que couber[28].

Silva, em sua obra, considera que a Lei n.º 9.296/1996 deve ser aplicada analogicamente, no que couber, uma vez que tanto a interceptação telefônica como a ambiental são meios de obtenção de prova que acarretam a violação da intimidade e da vida privada do investigado[29]. É o posicionamento com o qual Marcelo Mendroni e Everton Zanella também compactuam, desde um ponto de vista pragmático: como não possui procedimento probatório próprio, resta à interceptação ambiental seguir a mesma lógica da interceptação telefônica[30]. Tal posicionamento vai ao encontro do entendimento do legislador, conforme já dito, previsto na exposição de motivos do projeto original da Lei n.º 12.850/2013, pela desnecessidade de procedimento específico frente ao fato de a matéria estar supostamente suficientemente prevista na Lei n.º 9.296/1996.

---

[28] Em sentido favorável: SILVA, Eduardo Araujo da. *Crime Organizado:* procedimento probatório. 2ª ed. São Paulo: Atlas, 2009. p. 111. No sentido contrário: ARANTES FILHO, Marcio Geraldo Britto. *A interceptação de comunicação entre pessoas presentes*. Brasília: Gazeta Jurídica, 2013. p. 288-296; BADARÓ, Gustavo. *Processo Penal*. 4ª ed. São Paulo: Revista dos Tribunais, 2015. p. 506; MALAN, Diogo. Da Captação Ambiental de sinais eletromagnéticos, óticos, ou acústicos e os limites relativos à privacidade. AMBOS, Kai; ROMERO, Eneas (coord.). *Crime Organizado:* Análise da Lei 12. 850/2013. São Paulo: Marcial Pons, 2017. p. 51-81. p. 60-61.

[29] SILVA, Eduardo Araujo da. *Crime Organizado:* procedimento probatório. 2ª ed. São Paulo: Atlas, 2009. p. 111.

[30] MENDRONI, Marcelo Batlouni. *Crime organizado:* aspectos gerais e mecanismos legais. 6ª ed. Rio de Janeiro: Forense; São Paulo: Atlas, 2016. p. 246-247 e ZANELLA, Everton Luiz. *Infiltração de agentes no combate ao crime organizado*: análise do mecanismo probatório sob o enfoque da eficiência e o garantismo. Curitiba: Juruá, 2016. p. 162-164.

Tais argumentos devem ser avaliados com cautela. Como se viu, a interceptação ambiental é um meio de investigação que impacta diversos direitos fundamentais, com potencial de ser mais invasivo que a interceptação telefônica, por mais que em ambos os casos os interesses violados sejam semelhantes - intimidade e vida privada do investigado. Além disso, a aceitação pragmática da interpretação analógica apenas evita, sem enfrentar, o problema jurídico (de se utilizar um meio de investigação atípico que afeta seriamente direitos fundamentais), o qual permanece. Ademais, há diferenças cabais de objeto e de meio operacional, que dificultam a aplicação analógica da Lei das Interceptações Telefônicas.

Em primeiro lugar, quanto ao objeto: uma interceptação telefônica versa sobre conversas mediadas por um aparelho telefônico, atingindo apenas uma parte das atividades de comunicação do investigado, isto é, aquelas que envolvem utilização do aparelho telefônico. Por sua vez, uma interceptação ambiental é voltada para conversas sem intermediação, entre pessoas presentes, e capta substancialmente e amplamente mais uma comunicação, abrangendo monólogos e outras conversas presenciais antes, durante ou depois de cada conversa telefônica que pode ter feito, podendo se estender não só a aspectos orais, mas também visuais e eletromagnéticos, enriquecendo ainda mais o universo de informações obtidas.

Em segundo lugar, quanto ao meio operacional de realizar a interceptação: enquanto na ambiental há necessidade de diligências anteriores, como o prévio ingresso dissimulado de agentes públicos no local para a instalação do equipamento necessário para captar os sinais acústicos, ópticos ou eletromagnéticos, na interceptação telefônica não há tal necessidade, já que ela ocorre, em geral, com o auxílio direto de empresas de telefonia. Não há na Lei n.º 9.296/1996 disciplina do meio operacional prévio, que pode inclusive ser em domicílio. Assim, essa fase anterior fica numa espécie de limbo jurídico[31], carecendo regulamentação em lei.

Nesse contexto, a interceptação ambiental mostra-se uma medida investigativa mais invasiva e que exige cuidados regulatórios específicos.

---

[31] MALAN, Diogo. Da Captação Ambiental de sinais eletromagnéticos, óticos, ou acústicos e os limites relativos à privacidade. AMBOS, Kai; ROMERO, Eneas (coord.). *Crime Organizado:* Análise da Lei 12. 850/2013. São Paulo: Marcial Pons, 2017. p. 51-81. p. 67.

A transposição de previsões como a do artigo 3º da Lei das Interceptações Telefônicas, que fala em decretação de ofício da medida, ou do artigo 4º, §1º, que permite, mesmo que excepcionalmente, o requerimento verbal, é criticável, tendo em vista o caráter excepcional e invasivo da privacidade da interceptação ambiental. Permitir decreto de ofício ou verbalmente impediria uma análise detida da fundamentação da decisão judicial, além de, no primeiro caso, chocar-se com o princípio acusatório. Mais do que isso, deixar a questão do prazo e de sua prorrogação, nos termos do artigo 5º, em aberto cria amplas possibilidades de uso irrazoável.

Sendo assim, mostra-se problemática e insuficiente a aplicação analógica da Lei n.º 9.296/1996 à interceptação ambiental na linha do entendimento de Malan e Arantes Filho[32], sobretudo de uma perspectiva garantista. Com efeito, na situação atual do instituto, fere o princípio da legalidade probatória a utilização dessa prova atípica que atinge direitos fundamentais e que não goza de procedimento que possa lhe ser analogicamente aplicado de forma apropriada, a fim de embasar a sua execução. Em regra, essa conclusão jurídica deveria significar que o magistrado, ao deparar-se com um requerimento policial ou ministerial de interceptação ambiental, deveria negá-lo, sob pena de ilicitude probatória e consequente nulidade do processo. Caso fosse aceita, deveria ser declarada nula e desentranhada dos autos.

2. REGULAMENTAÇÃO: AS LIÇÕES DO TRIBUNAL EUROPEU DE DIREITOS HUMANOS

No item anterior, concluímos que a interceptação ambiental afeta direitos fundamentais e que a Lei de Interceptações Telefônicas se mostra inapta para ser aplicada analogicamente. Vimos também que a jurisprudência brasileira admite tal medida, sempre que autorizada judicialmente. No entanto, isso não significa que o instituto deva ficar

[32] C.f. MALAN, Diogo. Da Captação Ambiental de sinais eletromagnéticos, óticos, ou acústicos e os limites relativos à privacidade. AMBOS, Kai; ROMERO, Eneas (coord.). *Crime Organizado:* Análise da Lei 12. 850/2013. São Paulo: Marcial Pons, 2017. p. 51-81, p. 67 e ARANTES FILHO, Marcio Geraldo Britto. *A interceptação de comunicação entre pessoas presentes*. Brasília: Gazeta Jurídica, 2013. p 296.

sem regulamentação legislativa; pelo contrário, para coibir arbítrios do poder público que atentem a direitos constitucionalmente assegurados é que é necessário preencher a omissão legislativa nessa área.

Por conta disso, essa seção buscará na jurisprudência do Tribunal Europeu de Direitos Humanos quanto aos direito à vida privada e familiar, disposto no artigo 8º da Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais de 1950[33], lições para a regulamentação de interceptações ambientais. Acreditamos que ela oferece caminhos e orientações sobre o tipo de regime regulatório a que a medida deve estar submetida, bem como sobre o tipo de análise que deve ser feito a nível concreto para que possa ser deferida e utilizada de forma compatível com a proteção a direitos fundamentais.[34]

Por mais que haja um certo grau de autonomia dos países na regulamentação dos meios de investigação de provas ocultos, como é o caso da interceptação ambiental, é necessário que todos os procedimentos considerados invasivos ao direito consagrado no artigo 8º da Convenção sigam uma mesma base para evitar arbítrios[35], na forma delineada no ponto 8.2 do dispositivo.

---

[33] "*ARTIGO 8° Direito ao respeito pela vida privada e familiar*

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros."

[34] A escolha metodológica pelos julgados da Corte Europeia de Direitos Humanos se deu pelo fato de seus julgados constituírem paradigma na área de Direitos Humanos Internacional. Isso pode ser constatado quando, em julgados da Corte Interamericana de Direitos Humanos, por exemplo, decisões do TEDH são utilizadas como argumento de autoridade na fundamentação de conceitos que a própria CADH traz em seus casos. Vide o caso Escher e outros vs. Brasil, de 06 de julho de 2009, em que a CADH, ao tratar da legalidade da previsão das interceptações, utiliza dois casos da TEDH como referência para justificar a necessidade da lei clara e precisa sobre ingerências nos direitos humanos (CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Escher e outros vs. Brasil. Sentença de 06.07.09, Parágrafo 127. Disponível em <http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf>. Acesso em: 01 set. 2019).

[35] C.f. UBERTIS, Giulio. *Principi di Procedura Penale europea:* Le regole del giusto processo. 2ª ed. Milão: Rafaello Cortina Editore, 2009. p. 125 e ss.

Nesse contexto, segundo Malan, em suas decisões, o TEDH adota a seguinte metodologia: primeiramente, verifica se no caso em concreto houve real restrição ao direito à vida privada e familiar; se é identificada violação, a seguir a Corte examina se a medida restritiva utilizada estava em conformidade ou não com a legislação do Estado parte; tendo sido identificada violação ou não, o TEDH avaliará também, por fim, a necessidade daquela medida no âmbito de uma sociedade democrática[36] no caso concreto.

Assim, quanto aos requisitos específicos das medidas restritivas a direitos fundamentais, o primeiro está no próprio artigo 8.2 da Convenção: a reserva legal. Exige-se que o meio de investigação sigiloso tenha previsão legal dentro do Estado parte.

Quanto a este aspecto da legalidade, há três decisões relevantes do TEDH aos propósitos deste artigo e que foram proferidas no contexto de interceptações telefônicas. Segundo se depreende dos casos Valenzuela Contrera vs. Espanha[37], Kruslin vs. França[38] e Huvig vs. França[39], há uma delimitação do que se entende por previsão legal no ordenamento, a fim de regulamentar suficientemente os meios de investigação de prova que venham a ferir a privacidade. Para que atenda ao requisito da reserva legal, os seguintes aspectos devem ser observados: (i) determinação dos sujeitos que podem sofrer a interceptação da comunicação telefônica por decisão judicial; (ii) definição da natureza das infrações penais que autorizariam a utilização de tal medida; (iii) determinação do prazo de duração da interceptação; e (iv) criação dos procedimentos para a elaboração dos relatórios de transcrição, de encaminhamento da mídia original integral das gravações, intacta, para o juiz e para as partes, (para fins de controle da integridade da prova), além dos protocolos sobre as circunstâncias nas quais serão apagadas partes das gravações ou até destruída a mídia, especialmente quando houver sentença absolutória.

---

[36] MALAN, Diogo. Da Captação Ambiental de sinais eletromagnéticos, óticos, ou acústicos e os limites relativos à privacidade. AMBOS, Kai; ROMERO, Eneas (coord.). *Crime Organizado:* Análise da Lei 12. 850/2013. São Paulo: Marcial Pons, 2017. p. 51-81. p. 70-71.

[37] TEDH, caso Valenzuela Contrera vs. Espanha, julgado em 30.07.1998

[38] TEDH, caso Kruslin vs. França, julgado em 20.04.1990

[39] TEDH, caso Huvig vs. França, julgado em 20.04.1990

Baseado nesses *standards*, em 2000, o TEDH reconheceu violação ao artigo 8º no caso Khan vs. Reino Unido[40], no qual a polícia inglesa realizou uma interceptação domiciliar sem a devida regulamentação do instituto no ordenamento local. Como feriu a reserva legal, não havia como reconhecer a legalidade da captação de sinais acústicos dentro do domicílio do investigado.

Depois da reserva legal, deve ser analisada a estrita necessidade dessa medida no âmbito de uma sociedade democrática, nos termos do art. 8.2 da Convenção[41]. A análise é dividida em três requisitos: idoneidade, necessidade e proporcionalidade em sentido estrito. Quanto ao primeiro, exige-se que a medida seja apta ou adequada a atingir os objetivos propostos no caso concreto: proteção da segurança nacional, da segurança pública e do bem-estar econômico do país, defesa da ordem, prevenção das infrações penais, proteção da saúde ou da moral ou a proteção dos direitos e das liberdades de terceiros. No segundo ponto, deve ser avaliado se há medidas alternativas que menos restringem o direito à vida privada e familiar. No terceiro ponto, por sua vez, deve ser feita uma análise de ponderação de interesses conflitantes: entre o direito à vida íntima e familiar e as finalidades do artigo 8.2 que o Estado deve garantir em decorrência de uma persecução penal. A Corte então analisa no caso concreto se a intensidade da restrição ao direito guarda razoabilidade e proporcionalidade com a relevância do interesse perseguido pelo Estado.

Tudo isso deve ser acompanhado, conforme decisão tomada pelo TEDH, no caso Lambert vs. França[42], de instrumentos processuais idôneos para que o cidadão alvo de medida restritiva, como a interceptação ambiental, possa se defender. Na legislação do Estado parte, para que a medida possa ser considerada legal e proporcional, deve haver no ordenamento algum meio de controle processual da legalidade, seja ele uma nulidade a ser alegada, ou alguma forma de recurso por parte do investigado, a fim de evitar abusos em seu uso.

---

40 TEDH, Caso Khan vs. Reino Unido, julgado em 12.05.2000

41 MALAN, Diogo. Da Captação Ambiental de sinais eletromagnéticos, óticos, ou acústicos e os limites relativos à privacidade. AMBOS, Kai; ROMERO, Eneas (coord.). *Crime Organizado:* Análise da Lei 12.850/2013. São Paulo: Marcial Pons, 2017. p. 51-81. p. 72.

42 TEDH, Lambert vs. França, julgado em 24.08.1998

3. ANÁLISE DO PROJETO DE LEI ANTICRIME ENQUANTO TENTATIVA DE REGULAMENTAÇÃO

Tendo sida apresentada a jurisprudência do TEDH, volta-se a atenção ao Brasil. No início de 2019, o Ministro da Justiça Sérgio Moro apresentou um projeto de lei ao Congresso Nacional, cunhado de "Projeto Anticrime" (Projeto de Lei n.º 882/2019), com o intuito de recrudescer o combate a criminalidade, em especial a organizada. A proposta modificaria diversos diplomas legislativos brasileiros. Para o que nos interessa, altera a Lei n.º 12.850/2013, prevendo nova redação do artigo 3º sobre as hipóteses de cabimento dos meios de obtenção de prova previstos na lei, e inserindo os artigos 21-A e 21-B por meio da Seção VI, regulando a captação ambiental de sinais ópticos, acústicos e eletromagnéticos. Com base nas observações discutidas até aqui, essa seção analisa criticamente essa parte do projeto.

Atualmente, a redação prevista no artigo 3º permite o uso do rol de meios de obtenção de prova em qualquer fase da persecução penal, sem prejuízo de outros já previstos em lei. Ao não restringir o deferimento apenas à fase preliminar de investigação, o artigo não se atenta quanto ao caráter sigiloso e cautelar dos meios de obtenção de prova, que permite apenas a hipótese de contraditório diferido. Na ação penal, momento processual em que as partes já estão definidas e a produção de prova deve respeitar o contraditório pleno a fim de concretizar a ampla defesa do réu, não se pode permitir a investigação sub-reptícia, ao arrepio dos direitos e garantias processuais dele.

O Projeto Anticrime não corrige esse problema e ainda propõe uma nova redação[43] que aumenta o espectro de incidência para além dos crimes de organização criminosa. O texto legal proposto permite o uso dos meios de obtenção de prova lá previstos e, portanto, de interceptações ambientais, não apenas na investigação de infrações penais praticadas por organizações criminosas, mas também em todas aquelas cujas penas

[43] "Art. 3o Em qualquer fase da investigação ou da persecução penal de infrações penais praticadas por organizações criminosas, de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos ou de infrações penais conexas, serão permitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção da prova:"

máximas sejam superiores a quatro anos, ou em infrações conexas. Da perspectiva aqui avançada, considerando-se o nível de restrição a direitos fundamentais que interceptações ambientais podem acarretar e o contexto da reforma, o dispositivo deveria ser revisto para se conter apenas a crimes praticados por organização criminosa. Na forma como está, a proposta tem potencial de multiplicar diversos outros problemas do projeto para diversas outras investigações. É o que se passa a ver.

O *caput* do artigo 21-A[44] prevê a possibilidade do uso do meio de obtenção de prova na fase de investigação ou instrução criminal, desde que autorizada pela autoridade judicial, mediante requerimento da autoridade policial ou ministerial. Aqui temos uma escolha legislativa clara por permitir o requerimento direto pela autoridade policial, sem passar pelo crivo ministerial anterior. Ocorre que o Ministério Público é o titular da ação penal nos termos do artigo 129, I, da Constituição Federal e somente ele que pode avaliar se é o caso ou não de requerer tal medida para a obtenção da justa causa para o oferecimento da denúncia, representando quando encontrar necessidade, fundamentada, de que precisa de acervo probatório consistente a fim de dar subsidiariedade à denúncia. Assim, ao nosso ver, nos casos em que a autoridade policial se manifesta nesse sentido, o Ministério Público deveria ter de oferecer parecer endossando ou negando tal pedido endereçado ao juiz.

Nos incisos do artigo 21-A estão listadas as condições necessárias que precisam estar presentes para que a medida possa ser autorizada: (i) a prova não puder ser obtida por outros meios disponíveis e igualmente eficazes; (ii) houver elementos de prova razoáveis de autoria ou participação em infrações criminais cujas penas ultrapassam quatro anos ou em casos de infrações conexas. Como se depreende, traz dispositivo similar ao artigo 2º da Lei n.º 9.296/1996, com a diferença de que esta limita o uso da medida a investigações de crimes puníveis com reclusão, ao passo

[44] "Art. 21-A. Para investigação ou instrução criminal, poderá ser autorizada pelo juiz a requerimento da autoridade policial ou do Ministério Público a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, quando: I - a prova não puder ser feita por outros meios disponíveis e igualmente eficazes; e II - houver elementos probatórios razoáveis de autoria e participação em infrações criminais cujas penas máximas sejam superiores a quatro anos ou em infrações penais conexas."

que as interceptações ambientais estariam restritas aos crimes cuja pena máxima seja superior a quatro anos.

Nesta proposta de dispositivo, há avanços, diante da absoluta falta de regulamentação que a interceptação ambiental possui. O delineamento de requisitos hoje não existe na Lei n.º 12.850/2013, deixando espaços para arbítrios tanto na elaboração de pedidos quanto na concessão de autorizações judiciais e trazendo insegurança quando à legalidade da prova assim obtida. Assim, elencar requisitos formais e materiais é positivo. Dito isso, cabe notar que a lei não menciona explicitamente que a autorização judicial seja fundamentada. Não precisaria, já que se trata de comando obrigatório por força constitucional (art. 93, IX). Apesar disso, o reforço acentuaria a exigência de que a medida só pode ser utilizada quando efetivamente justificada. Neste aspecto, seria positivo se houvesse maior clareza quanto às etapas de fundamentação a que a decisão judicial deve atender para evitar que a medida seja deferida com base na menção de que os requisitos foram atendidos - algo como hoje existe no art. 10 da Resolução nº 59/2008 (na redação dada pela Resolução nº 217/2016) do CNJ para interceptações telefônicas, por exemplo. Também valeria a exigência explícita de que o contexto e a extensão da interceptação ambiental fossem delimitados de forma circunstanciada na decisão judicial.

Dando continuidade, o artigo possui seis parágrafos. O §1º[45] estipula que o requerimento ministerial ou policial deve descrever de modo detalhado o local e a forma de instalação do dispositivo de captação, enquanto o §2º[46] permite que a instalação do equipamento pode ser realizada, quando necessária, no período noturno ou por meio de operação policial disfarçada.

Esse conjunto de parágrafos merece análise detida. A mera menção a um procedimento prévio de inserção de equipamento e a exigência de que a autoridade policial ou o Ministério Público descrevam de modo detalhado o local e a forma de instalação do material de captação podem não ser suficientes para atender as preocupações discutidas anteriormente.

---

[45] "§1o O requerimento deverá descrever circunstanciadamente o local e a forma de instalação do dispositivo de captação ambiental."

[46] "§2o A instalação do dispositivo de captação ambiental poderá ser realizada, quando necessária, no período noturno ou por meio de operação policial disfarçada."

Melhor seria especificar e restringir, na própria lei, o agir da polícia quanto à instalação dos aparelhos de captação, impedindo excessos, especialmente nos casos mais invasivos - como o da interceptação ambiental domiciliar. A lei não baliza nem diferencia o que considera uma instalação legal de equipamentos em espaço público ou fechado, deixando isso a mercê da autoridade policial e do promotor de justiça, por exemplo.

Curiosa - e possivelmente mais temerária - é a expressão "*quando necessária*" presente no §2º. A instalação de equipamentos no período noturno ou mediante operação encoberta policial é medida de extrema gravidade, pois representa em si uma invasão e uma fraude. Nesse sentido, a entrada noturna ou sub-reptícia deveria estar melhor delimitada na lei, inserindo inclusive parâmetros mais específicos - como, por exemplo, a exigência de que fosse demonstrada a impossibilidade de instalação por outros modos e a apresentação de relatório circunstanciado acerca do modo de instalação, para permitir alguma instância de controle e responsabilização por eventuais abusos.

Nos termos do parágrafo §3º[47], a captação ambiental não pode ultrapassar quinze dias, podendo ser renovada por igual período mediante decisão judicial, frise-se, fundamentada, quando comprovadas (i) a imprescindibilidade da medida para a continuidade da investigação, e (ii) a presença de criminalidade permanente, habitual ou continuada. Trata-se de um avanço, dada a abertura que hoje existe.

Em seguida, o §4º[48] traz a figura da gravação clandestina feita por um dos interlocutores, sem autorização judicial prévia nem mesmo prévio conhecimento de autoridade policial ou ministerial. Tema antes restrito a decisões judiciais[49], o dispositivo legalizaria o instituto, desde

---

[47] "§3º A captação ambiental não poderá exceder o prazo de quinze dias, renovável por decisão judicial por iguais períodos, se comprovada a indispensabilidade do meio de prova e quando presente atividade criminal permanente, habitual ou continuada."

[48] §4º A captação ambiental feita por um dos interlocutores sem o prévio conhecimento da autoridade policial ou do Ministério Público poderá ser utilizada como prova de infração criminal quando demonstrada a integridade da gravação."

[49] O Supremo Tribunal Federal, em repercussão geral reconhecida na Questão de Ordem do RE 583937, de relatoria do Ministro Cezar Peluso, julgado em 19/11/2009, decidiu pela licitude da utilização da gravação clandestina por

que comprovada a integridade da gravação. Entretanto, vale observar que, na jurisprudência, era permitida a utilização como prova apenas em favor do interlocutor que realizou a gravação, em prol do seu direito de defesa, e para compor conduta criminosa alheia, como nos casos de extorsão, por exemplo, quando a vítima grava o autor sem o seu conhecimento a fim de demonstrar para as autoridades policiais a ocorrência do crime. Entendemos que o mesmo entendimento deve ser mantido na interpretação deste parágrafo, sempre de maneira restritiva.

Por sua vez, o §5º[50] prevê que se aplicam os artigos da Lei de Interceptações Telefônicas ao disposto no artigo 21-A de interceptação ambiental. Conforme visto, entendemos que essa aplicação estaria restrita apenas àquilo que for cabível e não atentar contra direitos fundamentais, uma vez que o uso de analogia nesses casos esbarra em uma série de problemas. De todo modo, vale apontar que a extensão por analogia importa para as interceptações ambientais alguns problemas já presentes na Lei n.º 9.296/1996[51]: para ficar em um exemplo, cabe citar a questão do incidente de inutilização de gravações que não interessem à prova acusatória. O parágrafo único do art. 9º daquela lei determina que o incidente deve ser assistido pelo *parquet*, mas a presença do acusado ou de seu representante legal é facultativa. Essa opção legislativa é alvo de críticas, uma vez que a discussão de retirada ou não de trechos da conversa interceptada, para que tenha legitimidade frente aos ditames constitucionais, deveria ser feita sempre sob a égide do contraditório[52],

---

uma das partes, consolidando o Tema 237, e a tese de que quando feita por um dos interlocutores, sem conhecimento dos outros, a prova é lícita.

[50] "§ 5º Aplicam-se subsidiariamente à captação ambiental as regras previstas na legislação específica para a interceptação telefônica e telemática."

[51] Outras questões em aberto são discutidas, por exemplo, em: SANTORO, Antonio E. R.; TAVARES, Natália L. F.; GOMES, Jefferson C. O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 3, n. 2, p. 605-632, mai./ago., 2017. https:/doi.org/10.22197/rbdpp.v3i2.76.

[52] MALAN, Diogo. Da Captação Ambiental de sinais eletromagnéticos, óticos, ou acústicos e os limites relativos à privacidade. AMBOS, Kai; ROMERO, Eneas (coord.). *Crime Organizado:* Análise da Lei 12. 850/2013. São Paulo: Marcial Pons, 2017. p. 51-81. p. 61. e BADARÓ, Gustavo. *Processo Penal*. 4ª ed. São Paulo: Revista dos Tribunais, 2015. p. 519.

com a presença pelo menos da defesa técnica do investigado, a fim de impedir que conversas sem relação com os fatos, de caráter íntimo, sejam juntadas aos autos. Isso permitiria inclusive que terceiro, vindo a saber de conversas suas interceptadas com o investigado, seja tomando conhecimento pelo próprio, ou pelo seu defensor, pudesse requisitar a inutilização do trecho caso não seja útil ao acervo probatório[53]. Nesse contexto, a imposição da aplicação analógica da Lei n.º 9.296/1996 às captações ambientais deixa de corrigir velhos problemas: ao invés de aproveitar a oportunidade para garantir acesso pela defesa técnica ao incidente de inutilização no caso de interceptações ambientais, a fim de que se possa exercer o contraditório e impedir que conversas sem conteúdo relevante para com a investigação sejam juntadas expondo a intimidade dos interlocutores desarrazoadamente, apenas se expande uma fragilidade de modelo regulatório atual.

Feita essa observação e voltando ao projeto, no §6º[54] do art. 21-A há previsão de que não há necessidade de decisão judicial nos casos em que houver a interceptação ambiental óptica em locais abertos ao público. A restrição contida no texto é de que a permissão se aplica a captações exclusivamente ópticas - não podendo abranger sinais acústicos, o que é uma limitação bem-vinda. Ainda assim, falta aqui um cuidado maior. O dispositivo trabalha com a velha (e ultrapassada) noção de que não existe privacidade em ambientes públicos e, diante da emergência do direito à autodeterminação informacional, que resguarda indivíduos também em público, tentar dar completa imunidade à medida. Assim confere, de modo criticável[55], ampla discricionariedade à autoridade policial, que não teria de comprovar indícios de envolvimento de alvos em quaisquer atividades criminosas nem prestar contas dessa diligência. De todo modo,

---

[53] BADARÓ, Gustavo. *Processo Penal*. 4ª ed. São Paulo: Revista dos Tribunais, 2015. p. 519-520.

[54] "*§ 6º A captação ambiental de sinais ópticos em locais abertos ao público não depende de prévia autorização judicial*."

[55] Ver também ANTONIALLI, Dennys; FRAGOSO, Nathalie; MASSARO, Heloísa. Da investigação ao encarceramento: as propostas de incremento do uso da tecnologia no Projeto de Lei Anticrime. Disponível em: <https://www.ibccrim.org.br/boletim_artigo/6337-Da-investigacao-ao-encarceramento--as-propostas-de-incremento-do-uso-da-tecnologia-no-Projeto-de-Lei-Anticrime.>. Acesso em: 01 set. 2019.

em qualquer leitura, não se pode extrair desse dispositivo uma autorização para usos irrestritos e sem balizas de câmeras com reconhecimento facial em áreas públicas, por exemplo. O uso desse tipo de ferramenta em si, pelos problemas específicos de vieses e falsos positivos, deve ser cuidadosamente debatido e apenas eventualmente regulamentado,[56] de modo que a alteração da redação para uma manifestação clara nesse sentido pode demonstrar mais respeito a direitos.

Por fim, o artigo 21-B[57] prevê um novo tipo penal para as captações ambientais sem autorização judicial, quando permitida (aqui, abarcando o permissivo do §6º), com pena de reclusão de dois a quatro anos, e multa. O §1º exclui a ilicitude da pessoa que realiza a gravação clandestina. Já o §2º determina que incorre na mesma pena o funcionário público que descumpra a determinação de sigilo da captação ambiental ou revelar o conteúdo das gravações antes do sigilo ser levantado.

A proposta analisada para por aí. Mas é possível imaginar outros pontos que uma regulamentação deveria enfrentar, com base nos direitos fundamentais afetados: Quando é admissível a interceptação ambiental em recintos em que o acusado não tem domicílio? Qual proteção a ser dada a terceiros não diretamente suspeitos? Como lidar com a questão do sigilo profissional de certas categorias? A prova obtida por interceptação ambiental pode ser emprestada a processos cíveis, administrativos, eleitorais? Qual o tratamento a ser dado à mídia original da captação?

Ao lado desses pontos, alguns delineamentos realizados pelo Tribunal Europeu de Direitos Humanos nos julgamentos sobre meios de

---

[56] Para um sucinto panorama das discussões, ver BIONI, Bruno; RIELLI, Mariana; LUCIANO, Maria. Regulação de reconhecimento facial em São Francisco, Jota, 25 de junho de 2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/regulacao-de-reconhecimento-facial-em-sao-francisco-25062019. Acesso em: 08 set. 2019.

[57] "Art. 21-B. Realizar captação ambiental de sinais eletromagnéticos, ópticos ou acústicos para investigação ou instrução criminal sem autorização judicial, quando esta for exigida. Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. § 1º Não há crime se a captação é realizada por um dos interlocutores. § 2º Incorre na mesma pena o funcionário público que descumprir determinação de sigilo das investigações que envolvam a captação ambiental ou revelar o conteúdo das gravações enquanto mantido o sigilo judicial."

investigação de prova ocultos podem trazer interessantes contribuições quanto a uma possível regulamentação de uma potencial legislação sobre o instituto. A exigência de reserva legal, principalmente, para a medida atentatória a direitos fundamentais e a devida regulamentação legislativa para o procedimento são necessários para cumprir a garantia ao procedimento do investigado, em nome da segurança jurídica. Mais do que isso, exigir que haja na lei instrumentos de defesa para o cidadão investigado é importantíssimo para garantir a ampla defesa e o contraditório e evitar arbítrios estatais durante a investigação.

CONCLUSÃO

O presente artigo analisou o status das interceptações ambientais como medida investigativa no direito brasileiro e identificou pontos que devem ser endereçados para que possa ser considerada compatível com direitos fundamentais. O diagnóstico, aqui limitado ao caso das interceptações ambientais, oferece um retrato de como instrumentos tecnológicos que estão sendo incorporados à prática do direito processual penal merecem detida análise de constitucionalidade e legalidade. Nesse sentido, vimos que a interceptação ambiental, enquanto meio de investigação de prova, é nominada na Lei n.º 12.850/2013, mas atípica, por não ter regulamentação específica na mesma lei ou em outra. Pelas suas especificidades, em respeito a direitos fundamentais, consideramos que não é suficiente a aplicação análoga da Lei n.º 9.296/1996 nem muito menos a mera existência de autorização judicial para que a medida seja válida. Contudo, isso não têm impedido que a medida seja declarada legal pela jurisprudência.

A seguir, voltamo-nos à jurisprudência e lições do Tribunal Europeu de Direitos Humanos com relação a restrições ao direito à vida privada e à interceptação ambiental para encontrar referências acerca dos ajustes que devem ser feitos no quadro regulatório e na prática jurídica brasileira. Como se viu, o Tribunal destaca o princípio da reserva legal: interceptações ambientais devem ser objeto de cuidadosa regulamentação. Em casos concretos, a aplicação dos parâmetros legais deve ser combinada com uma análise rigorosa da pertinência e da proporcionalidade da medida.

Por fim, verificamos que o Projeto de Lei Anticrime traz diversos elementos que podem ser vistos como avanços - notadamente porque hoje não há nada além do que menção à medida em lei. Assim, o fato de que se propõe elencar requisitos formais e materiais, por exemplo, já é um progresso. Ao mesmo tempo, o projeto é tímido no seu esforço de demonstrar um comprometimento com direitos fundamentais e é quase integralmente permeado por problemas que podem levar ao ou agravar o descontrole sobre o uso da medida. Nesse cenário, o caso das interceptações ambientais ensina que, para se elevar à revolução tecnológica sem admitir erosão de direitos, a prática jurídica brasileira tem um longo caminho a percorrer.

BIBLIOGRAFIA

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *Vigilância sobre as comunicações no Brasil:* interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. InternetLab: São Paulo, 2017.

ALEXY, Robert. *Teoria dos Direitos Fundamentais*. 2ª ed. São Paulo: Malheiros, 2015.

ALEXY, Robert. Constitutional Rights and Proportionality. *Revus (Online)*, v. 22, p. 51-65, 2014. Disponível em: <http://revus.revues.org/2783>. Acesso em: 01. set. 2019. https://doi.org/10.4000/revus.2783

ANTONIALLI, Dennys; FRAGOSO, Nathalie; MASSARO, Heloísa. Da investigação ao encarceramento: as propostas de incremento do uso da tecnologia no Projeto de Lei Anticrime. Disponível em: <https://www.ibccrim.org.br/boletim_artigo/6337-Da-investigacao-ao-encarceramento-as-propostas-de-incremento-do-uso-da-tecnologia-no-Projeto-de-Lei-Anticrime.>. Acesso em: 01 set. 2019.

ARANTES FILHO, Marcio Geraldo Britto. *A interceptação de comunicação entre pessoas presentes*. Brasília: Gazeta Jurídica, 2013.

ARANHA, Adalberto José de Camargo. *Da Prova no Processo Penal*. 7ª ed. São Paulo: Saraiva, 2008.

AVOLIO, Luis Francisco. *Provas ilícitas*: interceptações telefônicas, ambientais e gravações clandestinas. 3ª ed. São Paulo: Revista dos Tribunais, 2003.

BADARÓ, Gustavo. Editorial do dossiê "Prova penal: fundamentos epistemológicos e jurídicos". *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 4, n. 1, p. 43-80, 2018. http://dx.doi.org/10.22197/rbdpp.v4i1.138

BADARÓ, Gustavo. Hipóteses que autorizam o emprego de meios excepcionais de obtenção de prova. In: AMOS, Kai; ROMERO, Eneas (orgs.). *Crime Organizado:* Análise da Lei 12.850/13. Marcial Pons: Madri, 2017. p. 13-49.

BADARÓ, Gustavo. Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia. In: LIMA, José Corrêa de; CASARA, R. R. Rubens. (coord.). *Temas para uma perspectiva crítica do direito:* homenagem ao Professor Geraldo Prado. Rio de Janeiro: Lumen Juris, 2010. p. 483-499.

BADARÓ, Gustavo. *Processo Penal*. 4ª ed. São Paulo: Revista dos Tribunais, 2015.

BIONI, Bruno; RIELLI, Mariana; LUCIANO, Maria. Regulação de reconhecimento facial em São Francisco, Jota, 25 de junho de 2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/regulacao-de-reconhecimento-facial-em-sao-francisco-25062019. Acesso em: 08 set. 2019

CABETTE, Eduardo Luiz Santos. Gravações Clandestinas e Ambientais: tutela constitucional da intimidade e os agentes públicos. *Boletim IBCCRIM*, São Paulo, n. 65, p. 5-6, 1998.

CARMONA, Claudia. Le intercettazioni ambientali in relazione allá normative del 1991 sui reati di criminalità organizata. *Rivista Italiana di Diritto e Procedura Penale*, v. 42, n.1, p. 352-358, 1999.

CUNHA JÚNIOR, Dirley da. *Curso de Direito Constitucional*. 7ª ed. Salvador: Juspodivm, 2013.

DEZEM, Guilherme Madeira. *Da prova penal:* tipo processual, provas típicas e atípicas: (atualizado de acordo com as Leis 11.689/08, 11.690/08 e 11.719/08). Campinas: Millenium, 2008.

DEZEM, Guilherme Madeira. *Curso de Processo Penal*. São Paulo: Revista dos Tribunais, 2015.

MARTINO, Corrada di. Le intercettazioni ambientali. *L'Indice Penale*, Verona, v. 6, n. 3, p. 1.147-1.171, set./dez. 2003.

FERRAZ JR., Tercio Sampaio, Sigilo de Dados: o direito à privacidade e os limites da função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo,* São Paulo, v. 88, p. 439-459, 1993.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006.

GRINOVER, Ada Pellegrini; GOMES FILHO, Antonio Magalhães; FERNANDES, Antonio Scarance. *As nulidades no processo penal.* 11ª ed. São Paulo: Revista dos Tribunais, 2009.

HAIRABEDIÁN, Maximiliano. La grabación como prueba en el proceso penal. *Pensamiento penal y criminológico: Revista de derecho penal integrado*, Córdoba, v. 3, n. 4, p. 119-150, 2002.

FERNANDES, Antonio Scarance. O equilíbrio entre a eficiência e o garantismo e o crime organizado. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 16, n. 70, p. 229-268, jan./fev. 2009.

FERNANDES, Antonio Scarance. *Teoria Geral do Procedimento e o Procedimento no Processo Penal*. São Paulo: Revista dos Tribunais, 2005.

FONSECA, Tiago Abud da. *Interceptação telefônica:* a devassa em nome da lei. Rio de Janeiro: Espaço Jurídico, 2008.

GOMES, Luiz Flávio. *Interceptação telefônica:* comentários à lei 9.296, de 24.07.1996. 2ª ed. São Paulo: Revista dos Tribunais, 2013.

GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flavio Luiz; MORAES, Maurício Zanoide de (orgs.). *Estudos em homenagem à professora Ada Pellegrini Grinover*. São Paulo: DPJ, 2005. p. 303-318.

GOMES FILHO, Antonio Magalhães; BADARÓ, Gustavo. Prova e sucedâneos da prova no processo penal brasileiro. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 15, n. 65, p. 175-208, mar./abr. 2007.

GRECO FILHO, Vicente. *Interceptação telefônica:* considerações sobre a lei n. 9.296, de 24 de julho de 1996. 2ª ed. rev. São Paulo: Saraiva, 2005.

LOPES JÚNIOR, Aury. *Direito Processual Penal*. 9ª ed. São Paulo: Saraiva, 2012.

MALAN, Diogo. *Da captação ambiental de sinais eletromagnéticos, óticos ou acústicos e os limites relativos à privacidade* In: AMBOS, Kai; ROMERO, Eneas (orgs.). *Crime Organizado:* Análise da Lei 12.850/13. Marcial Pons: Madri, 2017. p. 51-81.

MALAN, Diogo. I*nterceptação de comunicações telefônicas:* standards dos sistemas interamericano e europeu de direitos humanos. In: SANTORO, Eduardo R. S.; MADURO, Flávio M. *Interceptação telefônica:* 20 anos da Lei 9.296/96. Belo Horizonte: Editora D'Plácido, 2016. p. 149-174.

MALAN, Diogo. Pro*cesso Penal do Inimigo*. *Revista Brasileira de Ciências Criminais*, v. 14, n. 59, p. 223-258, mar./abr. 2006.

MASSON, Cleber; MARÇAL, Vinícius. *Crime Organizado*. 3ª ed. Rio de Janeiro: Forense; São Paulo: Método, 2017.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*. São Paulo: Saraiva, 2014.

MENDRONI, Marcelo Batlouni. *Crime organizado:* aspectos gerais e mecanismos legais. 6ª ed. Rio de Janeiro: Forense; São Paulo: Atlas, 2016.

MOORE, Adam D. *Privacy Rights:* Moral and Legal Foundations. Pennsylvania: Penn State University, 2010.

MUÑOZ CONDE, Francisco. *Valoración de las grabaciones audiovisuales em el proceso penal*. 2ª ed. Buenos Aires: Hammurabi, 2007.

NUCCI, Guilherme de Souza. *Organização criminosa:* Comentários à Lei 12.850, de 2 de agosto de 2013. São Paulo: Revista dos Tribunais, 2013.

NUCCI, Guilherme de Souza. *Leis Penais e Processuais Penais Comentadas*. v. 1. 10ª ed. Rio de Janeiro: Forense, 2017.

PRADO, Geraldo. *Limites às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça*. Rio de Janeiro: Lumen Juris, 2005.

RANGEL, Paulo. *Direito Processual Penal*. 18ª ed. Rio de janeiro: Lumen Juris, 2011.

RANGEL, Ricardo Melchior de Barros. *A prova ilícita e a interceptação telefônica no direito processual penal brasileiro*. Rio de Janeiro: Forense, 2000.

ROXIN, Claus. *La proibición de autoincriminación y de las escuchas domiciliarias*. Trad. Francisco Muñoz Conde. Buenos Aires: Hammurabi, 2008.

SANTORO, Antonio E. R.; TAVARES, Natália L. F.; GOMES, Jefferson C. O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 3, n. 2, p. 605-632, mai./ago. 2017. https://doi.org/10.22197/rbdpp.v3i2.76.

SIDI, Ricardo. A interceptação das comunicações telemáticas no processo penal. Belo Horizonte: D'Plácido, 2016.

SILVA, Eduardo Araújo da. *Organizações criminosas:* aspectos penais e processuais penais da Lei 12.850/13. 2ª ed. São Paulo: Atlas, 2017.

SILVA, José Afonso. *Curso de Direito Constitucional*. 32ª Ed. São Paulo: Malheiros, 2009.

UBERTIS, Giulio. *Principi di Procedura Penale europea:* Le regole del giusto processo. 2ª ed. Milão: Rafaello Cortina Editore, 2009.

ZANELLA, Everton Luiz. *Infiltração de agentes no combate ao crime organizado:* análise do mecanismo probatório sob o enfoque da eficiência e o garantismo. Curitiba: Juruá, 2016.

Informações adicionais e declarações dos autores (*integridade científica*)

Declaração de conflito de interesses (conflict of interest declaration): os autores confirmam que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

- *Jacqueline de Souza Abreu*: projeto e esboço inicial, levantamento bibliográfico, revisão bibliográfica, redação, revisão crítica com contribuições substanciais, aprovação da versão final.

- *Gianluca Martins Smanio*: projeto e esboço inicial, levantamento bibliográfico, revisão bibliográfica, redação, revisão crítica com contribuições substanciais, aprovação da versão final.

Declaração de ineditismo e originalidade (declaration of originality): os autores asseguram que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atestam que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 10/07/2019
- Controle preliminar e verificação de plágio: 12/07/2019
- Avaliação 1: 24/07/2019
- Avaliação 2: 25/07/2019
- Avaliação 3: 27/07/2019
- Decisão editorial preliminar: 27/08/2019
- Retorno rodada de correções: 08/09/2019
- Decisão editorial final: 20/09/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editora-associada: 1 (CC)
- Revisores: 3

COMO CITAR ESTE ARTIGO:

ABREU, Jacqueline de S.; SMANIO, Gianluca M. Compatibilizando o uso de tecnologia em investigações com direitos fundamentais: o caso das interceptações ambientais. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1449-1482, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.262

A infiltração online no processo penal – Notícia sobre a experiência alemã

The Online Search in the Criminal Procedure Law – About the German Experience

Luís Greco[1]

Universidade Humboldt - Berlim, Alemanha

luis.greco@rewi.hu-berlin.de

https://orcid.org/0000-0003-3087-4561

Orlandino Gleizer[2]

Universidade Humboldt - Berlim, Alemanha

gleizero@student.hu-berlin.de

http://lattes.cnpq.br/5773080132816841

https://orcid.org/0000-0002-4877-748X

Resumo: O artigo descreve a discussão alemã sobre a técnica de investigação da infiltração online no processo penal e tenta extrair lições para o sistema brasileiro.

Palavras-chave: infiltração online; processo penal; direitos fundamentais; direito alemão.

[1] Professor Catedrático de Direito Penal, Direito Processual Penal e Direito Penal Estrangeiro e Teoria do Direito Penal da Universidade Humboldt, de Berlim, Alemanha. Habilitação em direito penal na Universidade Ludwig Maximilian, de Munique, Alemanha; doutor em direito e LL.M. na mesma instituição.

[2] Doutorando em Ciência do Direito pela Universidade Humboldt de Berlim; LL.M pela Universidade de Augsburg (Alemanha); mestre em Direito Penal pela Universidade do Estado do Rio de Janeiro. Advogado criminal; assistente científico junto à cátedra do Prof. Dr. Dr. Eric Hilgendorf, na Universidade Julius Maximiliam de Würzburg (Alemanha).

Abstract: *The article describes the German discussion about the online-infiltration as a fact-finding measure in Criminal Procedure and tries to learn some lessons for the Brazilian system.*

Keywords: *online search; criminal procedure; fundamental rights; German law.*

I. Introdução

Pode o Estado acessar nossos computadores remotamente, sem nosso conhecimento, com a finalidade de, vasculhando o conteúdo ali disponível, obter prova de crimes? Se sim, diante de que pressupostos? É dessas duas perguntas, sobre a legitimidade abstrata e concreta daquilo que no presente trabalho chamaremos de *infiltração online*, e que na Alemanha é conhecido como Online-Durchsuchung – o que seria mais literalmente de traduzir-se como "busca online" – que cuidaremos no presente artigo. A primeira delas, veremos, receberá uma resposta clara e definitiva: no Direito brasileiro, inexiste legitimação para essa medida. A experiência alemã será descrita em detalhe, sobretudo no que diz respeito à segunda pergunta, isto é, aos pressupostos da infiltração, a fim de oferecer elementos para um debate sobre uma eventual introdução da medida no Brasil.

Nossas reflexões terão, por primeiro passo, uma recapitulação da dogmática dos direitos fundamentais, que demarca âmbitos da vida em que o Estado só pode adentrar observando pressupostos relativamente severos (II.). Passaremos a uma análise mais detida da infiltração online, em que descreveremos as dimensões em que ela configura uma intervenção em direito fundamental, levando em conta especialmente o novo direito fundamental, cunhado pelo Tribunal Constitucional Federal alemão (Bundesverfassungsgericht – BVerfG), à integridade e confiabilidade de sistemas informáticos (III.). Depois de um breve retorno ao direito brasileiro (IV.), em que verificaremos a impossibilidade da medida segundo a *lex lata*, daremos notícia do regime da infiltração online no direito alemão, porque cremos que ele pode servir como linha de orientação para uma eventual legislação brasileira sobre o tema (V.). Por fim, mencionaremos três pontos controvertidos na Alemanha, conferindo especial atenção às dúvidas sobre a constitucionalidade da nova lei (VI.).

II. Considerações prévias sobre justificação de intervenções em direitos fundamentais

1. Antes de nos voltarmos à medida da infiltração online, é preciso assentar algumas premissas sobre os limites à atuação do Estado em um regime que conhece direitos fundamentais, tal qual o brasileiro. A Constituição Federal brasileira assegura aos indivíduos direitos fundamentais oponíveis contra todos os poderes do Estado – Executivo, Legislativo e Judiciário (cf., especialmente, o art. 5º CF). Isso significa, inquestionavelmente, que o Estado não pode tudo contra o indivíduo; há espaços em que, em princípio, o Estado não pode adentrar, e esses espaços chamam-se *direitos fundamentais*. Diante do imperativo jurídico de proteger os indivíduos e a sociedade e de promover os fins que lhe incumbem (por ex., art. 3º CF), o Estado pode ver-se forçado a adentrar nesses espaços individuais protegidos. Para tanto, ele necessitará de uma *justificação especial*.

Dessas ideias um tanto simples derivam os conceitos básicos da teoria dos direitos fundamentais que manejaremos no curso do presente artigo.[3] Esses conceitos, elaborados pelo constitucionalismo alemão, vêm aos poucos encontrando eco na doutrina brasileira.[4] O espaço demarcado por cada direito fundamental, aquele setor da vida objeto da proteção especial, chama-se *âmbito de proteção* do direito fundamental; aqui terá início a nossa análise. O comportamento estatal que impossibilita ou dificulta a prática de algo que se insere no âmbito de proteção é uma *intervenção* – a segunda etapa da análise. Toda intervenção estatal deve estar *justificada* – o que se examinará em terceiro lugar. Caso essa justificação

---

[3] Para um panorama desse "processo penal constitucional" alemão *Greco*, Introdução in: *Wolter*, O inviolável e o intocável no direito processual penal: reflexões sobre a dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal, São Paulo, 2018, p. 30 e ss.

[4] *Ferreira Mendes*, Limitações dos direitos fundamentais, in: Ferreira Mendes/Gonet Branco, Curso de Direito Constitucional, 12ª. ed., 2017, p. 190 e ss.; *Sarlet*, Teoria geral dos direitos fundamentais, in: Sarlet/Marinoni/Mitidiero, Curso de direito constitucional, 7ª. ed., 2018, p. 305 e ss. (385 e ss.); *Dimoulis/Martins,* Teoria Geral dos Direitos Fundamentais, 5ª. ed., 2014, p. 129 e ss.

não possa ser afirmada, qualifica-se a intervenção de *violação* ao direito fundamental. Violações são intervenções não justificadas, portanto ilícitas.

2. Detenhamo-nos a essa terceira etapa, a da *justificação*. Há, pelo menos, três pressupostos de relevância geral – ou seja, pertinentes a todos os direitos fundamentais – a serem respeitados: um, de natureza formal, é a existência de um fundamento legal; os outros dois, materiais, consistem em que a intervenção não afete o conteúdo essencial/de dignidade desses direitos e seja proporcional.

a) O limite formal, de que direitos fundamentais estão submetidos a uma *reserva de lei*, encontra-se constitucionalmente positivado (art. 5º II CF): "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei".[5] O Executivo e também o Judiciário precisam de um fundamento legal, que é o que os autoriza a agir contra os cidadãos. Porque, numa democracia, em que "todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente" (art. 1º parágrafo único CF), é apenas o povo quem pode autorizar, por meio de seu consentimento expressado através das leis votadas e aprovadas por seus representantes, o exercício do poder de intervir.

Aqui, parecem-nos relevantes cinco rápidas observações. Os direitos fundamentais protegem o cidadão não apenas do Executivo, das instâncias de persecução, mas também dos juízes; isso significa que, onde inexistir lei prevendo uma intervenção, é descabida a discussão se ela é possível mediante autorização judicial. A lei não regula intervenção, mas a *fundamenta, autoriza, torna juridicamente possível*.[6] Por isso também é descabido justificar intervenções no slogan de que não há direitos absolutos ou na proporcionalidade, dispensando uma lei; ainda que isso fosse correto,[7] não cabe intervenção sem lei que a autoriza. Além disso,

---

[5] Em detalhe sobre a reserva de lei e o que daí decorre para o processo penal, *Greco* (nota 3), p. 36 e ss.

[6] *Greco* (nota 3), p. 40.

[7] Pensamos que o direito de não ser torturado é absoluto (cf. *Greco*, As regras por trás da exceção: reflexões sobre a tortura nos chamados "casos de bomba-relógio", in: RBCC 78 [2009], p. 7 e ss.); assim também o é o direito de não ser escravizado. O slogan de que inexistem direitos absolutos implica em um questionamento da própria ideia de dignidade humana, fundamento também da ordem constitucional brasileira (art. 1º III CF). Sobre a dignidade humana no direito brasileiro, especialmente sobre a discussão em torno da

a lei deve ser precisa (*mandato de determinação*) – cláusulas gerais de autorização só permitem intervenções bagatelares –, com o que se torna inadmissível estender seu alcance a hipóteses não expressamente previstas (*proibição de analogia*). Por fim, observe-se que da mera competência para a realização de uma tarefa (como investigar, acusar ou julgar) não se pode derivar qualquer autorização para intervir em esferas protegidas (*distinção entre normas de competência entre e normas autorizitativas*).[8]

b) Um primeiro limite material é o de que a intervenção estatal não pode atingir o núcleo dos direitos fundamentais, o que tradicionalmente se chama de *conteúdo essencial* [Wesensgehalt] ou *de dignidade*.[9] Esse núcleo do direito fundamental é *intocável*; qualquer intervenção já implica em uma violação.[10] Essa ideia poderia ser exemplificada da seguinte forma: enquanto trancar alguém em uma cela de prisão representa uma intervenção justificável no direito fundamental à liberdade de locomoção (art. 5º XV CF), colocar essa pessoa em uma prisão perpétua impassível de ser revista afetaria a liberdade em seu âmago e, com isso, a dignidade humana.[11]

c) Por fim, o terceiro requisito geral de justificação de uma intervenção em direito fundamental é a *proporcionalidade*, uma barreira que os direitos fundamentais de defesa levantam também contra o próprio legislador, submetendo-o a *limites* na imposição de *limites* ao gozo dos direitos fundamentais ("limites dos limites").[12] A ideia da proporcionalidade é verificar, por meio de diferentes critérios, a harmonia entre o propósito (constitucionalmente legítimo) do legislador e o grau de afetação da esfera individual, em uma relação meio-fim. A intervenção tem de ser idônea, necessária e adequada para a promoção desse fim. É esse

---

possibilidade de relativizá-la, *Sarlet*, Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988, 10ª. ed. Porto Alegre, 2015, item 6.2 e ss.

8 *Greco* (nota 3), p. 37 e ss.

9 A rigor, estamos procedendo a uma simplificação: nem sempre se identifica conteúdo essencial e conteúdo de dignidade, cf. com referências *Greco* (nota 3), p. 35.

10 *Greco* (nota 3), p. 32.

11 *Greco* (nota 3), p. 35.

12 Cf., por todos, *Sarlet* (nota 4), p. 394 ss.

o nível mais complexo da operacionalização dogmática da justificação de intervenções em direitos fundamentais, já que aqui assumem relevância considerações das mais diversas ordens.

III. A infiltração online enquanto intervenção em direitos fundamentais da perspectiva do direito alemão

1. Desenvolvimento da infiltração online no direito alemão

A possibilidade da infiltração estatal, oculta e remota, em dispositivos informáticos para a investigação de crimes começou a ser discutida pelos tribunais alemães por volta de 2006. Em um primeiro momento, houve tentativas de utilização desse método oculto de investigação com base em aplicações extensivas ou mesmo analógicas de três normas do ordenamento jurídico alemão: aquelas que autorizavam a apreensão de objetos com finalidade investigativa (§ 94 Código de Processo Penal alemão – Strafprozessordnung, StPO), a de busca domiciliar (§ 102 StPO) e do monitoramento de telecomunicações (§ 100a StPO).

a) A decisão do Bundesgerichtshof de 2007 (BGHSt 51, 211)

Após os primeiros casos chegarem ao *Bundesgerichtshof* (tribunal alemão equivalente a nosso STJ, doravante BGH), a Corte, em 2007, entendeu não haver fundamento legal para a invasão de computadores, e que uma analogia tampouco seria possível.[13] Em síntese, estabeleceu-se, pela primeira vez, que o acesso aos dados armazenados no computador dos investigados seria uma severa intervenção ao direito fundamental à autodeterminação informacional – direito fundamental que o BVerfG já reconhecia desde 1983[14] – deduzido do direito ao livre desenvolvimento da personalidade e da dignidade humana (Art. 2 Abs. 1 c/c Art. 1 Abs. 1 Lei Fundamental, Grundgesetz – GG). A norma de autorização para

[13] BGHSt 51, 211.

[14] Cf. a decisão do censo, BVerfGE 65, 1; a respeito, em detalhe, *Greco* (nota 3), p. 41 e ss.

buscas domiciliares (§ 102 StPO) – um método de investigação físico, e não virtual – não autorizaria a medida, já que a busca em objetos físicos se baseia no princípio da publicidade: o investigado deve ser notificado e tem o direito de acompanhar a medida de busca em seu domicílio (§ 106 Abs. 1 Satz 2 StPO).[15] Tampouco as normas que autorizam intervenções ocultas alcançariam a medida.[16] A norma que autoriza o monitoramento de telecomunicações (§ 100a StPO) também não poderia ser aplicada ao caso: ainda que, durante a devassa nos dispositivos informáticos, possivelmente dados e procedimentos de telecomunicação sejam tangenciados, o objetivo central da medida seria a coleta abrangente de todas as informações armazenadas nos dispositivos, não necessariamente derivadas de telecomunicações.[17] De vigilância acústica domiciliar (§ 100c StPO) tampouco se trataria.[18] Por fim, a cláusula geral para investigações do Ministério Público e da Polícia (§ 161 StPO)[19] não abrangeria uma intervenção tão severa em direito fundamental.[20] O BGH também rechaça qualquer tentativa no sentido de fundamentar a medida combinando os elementos das várias normas, por violação da ideia de reserva de lei e do mandato de determinação.[21] E a publicação do julgado no repertório oficial conclui com uma frase a que a recepção brasileira da ideia de proporcionalidade deveria atentar: "O princípio da proporcionalidade limita, no caso concreto, as faculdades legalmente previstas, e não pode, portanto, substituir-se a um fundamento autorizativo que inexista."[22] *Não é a proporcionalidade, e sim a lei proporcional, que fundamenta intervenção em direito fundamental*.

Por isso, o tribunal afirmou que uma intervenção tão severa em direitos fundamentais de liberdade precisaria estar amparada por uma *norma autorizativa específica*, que, para ser constitucionalmente compatível, precisaria também se atentar aos severos pressupostos de intervenção

---

15 BGHSt 51, 211 (212 e ss., nm. 4 e ss.).

16 BGHSt 51, 211 (217 e ss., nm. 17 e ss.).

17 BGHSt 51, 211 (217 e ss., nm. 18).

18 BGHSt 51, 211 (218, nm. 19).

19 A respeito, *Greco* (nota 3), p. 39.

20 BGHSt 51, 211 (218, nm. 21).

21 BGHSt 51, 211 (219, nm. 22).

22 BGHSt 51, 211 (219, nm. 22).

exigidos pelo direito fundamental em questão. Ou seja, a medida carecia, até então, de *fundamento legal*.

b) A evolução posterior

Paralelamente à decisão do BGH, o estado alemão de Renânia do Norte-Vestfália inseriu, em sua Lei de Proteção à Constituição de 2006 [*Verfassungsschutzgesetz*] dispositivo que autorizaria a medida. A rigor, não se tratava aqui de processo penal, e sim de *direito dos serviços de inteligência*. No direito alemão, o Serviço de Proteção à Constituição realiza a atividade de inteligência estatal contra o extremismo político.[23] O direito de inteligência, cuja finalidade é a *coleta de informações* em momento prévio à existência de perigos, é um ramo autônomo, que não se confunde com o processo penal. Fala-se em um imperativo de separação [*Trennungsgebot*]: persecução e inteligência, direito processual penal (repressivo, fundado na suspeita) e o direito de inteligência (que se orienta pela precaução) não podem misturar-se, doutro modo, cair-se-ia na Gestapo.[24] A norma em questão não autorizava a infiltração online, portanto, com finalidade de busca de provas para o processo penal, mas para antecipar-se a crimes ainda não ocorridos.

Essa norma foi objeto, em 2008, da primeira decisão do BVerfG sobre a infiltração online.[25] Dentre outras coisas, a Corte declarou inconstitucional o dispositivo, criou um novo *direito fundamental à garantia da confiabilidade e integridade de sistemas informáticos*, derivando-o do direito geral de personalidade (Art. 2 Abs. 1 c/c Art. 1 Abs. 1 GG) e formulando os pressupostos materiais e procedimentais mínimos para a legitimidade da medida. Retornaremos a essa decisão fundamental logo em seguida (abaixo, 2.).

As exigências da corte serviram de base para a criação, em 2008, de norma autorizativa de infiltração online na Lei do Ofício Criminal

---

[23] Sobre o que segue *Greco* (nota 3), p. 51 e ss.

[24] O imperativo de separação separa também polícia preventiva e inteligência; o direito alemão conhece, assim, três níveis separados, o da polícia repressiva, o da polícia preventiva e o da inteligência.

[25] BVerfGE 120, 274.

Federal (Gesetz über das Bundeskriminalamt, BKA-Gesetz), uma lei de polícia preventiva, que não se aplica ao processo penal, de orientação repressiva.[26] Essa norma, então submetida a novo escrutínio da corte em 2016,[27] foi declarada parcialmente constitucional. Em 2017, o legislador criou norma autorizativa para a infiltração online como medida de investigação no processo penal (§ 100b StPO). A constitucionalidade dessa norma, por sua vez, encontra-se atualmente submetida a nova avaliação do BVerfG. Enquanto essa decisão é aguardada, as únicas considerações da corte sobre a infiltração online são aquelas relativas ao âmbito do direito de inteligência e do direito de polícia.

2. A infiltração online da perspectiva do BVerfG: o novo direito fundamental e suas exigências

a) A primeira conclusão alcançada pelo BVerfG na decisão sobre a Lei da Renânia do Norte-Vestfália foi a de que os direitos fundamentais dos Arts. 10 e 13 GG – que garantem proteção ao sigilo das telecomunicações e ao domicílio, respectivamente – não seriam aptos a proteger o indivíduo suficientemente contra o acesso a seus sistemas informáticos. O primeiro ponto de discussão localiza-se, portanto, no *âmbito de proteção* desses direitos fundamentais (sobre esse conceito, acima, II.). A pergunta é: o que protegem eles?

aa) O *Art. 10 GG*, na visão do BVerfG, protege a *telecomunicação* privada, garantindo a confiabilidade da comunicação entre indivíduos distantes entre si, em razão da maior vulnerabilidade a interceptações indevidas (especialmente, estatais).[28] O direito ao sigilo das telecomunicações, essencial para a proteção da privacidade, defende o indivíduo contra o levantamento não autorizado de informações e garante a privacidade à distância, de modo que comunicantes gozem do mesmo nível de privacidade que teriam em uma comunicação presencial. Por isso, ele protege, em última instância, o livre desenvolvimento da personalidade.[29]

---

[26] Cf. a nota 24.

[27] BVerfGE 141, 220.

[28] BVerfGE 120, 274 (306 e ss.).

[29] Cf. já BVerfGE 115, 166 (182).

A Corte entendeu, no entanto, que nem o acesso às informações nas mídias de armazenamento, nem o monitoramento da utilização de um sistema informático seriam intervenções à garantia de confiabilidade da telecomunicação do Art. 10 GG. E isso mesmo que a transferência dos dados obtidos nos dispositivos infiltrados até a central do investigador ocorresse por meio de sistemas de telecomunicação, como acontece com o acesso online em mídias de armazenamento de um computador alheio.[30]

bb) O *Art. 13 GG*, protetor da *inviolabilidade do domicílio*, garante ao indivíduo, com vistas à dignidade humana e ao interesse no desenvolvimento da personalidade, um espaço físico elementar de vida. O bem protegido desse direito fundamental é a esfera espacial na qual a vida privada se desenvolve.[31] Na visão do BVerfG, esse direito fundamental não seria pertinente, pois seu objeto de proteção seria uma componente espacial do âmbito privado, que não seria tangenciada, caso uma intervenção ocorresse fora do domicílio ou o local do dispositivo em questão (um laptop ou um smartphone) não fosse reconhecível durante a investigação. A utilização de uma conexão do dispositivo com a internet ou com um outro computador também não interferiria na esfera espacial da vida privada.[32]

cc) Por isso, o BVerfG entendeu que, para fazer frente aos especiais perigos ao livre desenvolvimento da personalidade na era digital, vinculados à utilização de computadores como dispositivos individuais ou como sistemas interconectados, seria necessário construir um *outro direito fundamental*, a ser derivado do direito geral de personalidade, por sua vez derivado de uma leitura conjunta do Art. 2 Abs. 1, que prevê o direito ao livre desenvolvimento da personalidade, e do Art. 1 Abs. 1 GG, que protege a dignidade humana.[33]

(1) Na ordem jurídica alemã, o *direito geral de personalidade* (Art. 2 Abs. 1 GG)[34] é um direito fundamental de alcance geral. Ele protege, na

---

30 BVerfGE 120, 274 (308).

31 Cf. já BVerfGE 89, 1 (12); 103, 142 (150 s.).

32 BVerfGE 120, 274 (309 e ss.).

33 BVerfGE 120, 274 (302 e ss.).

34 Art. 2 Abs. 1 GG: "... direito ao livre desenvolvimento da personalidade, desde que não se violem os direitos alheios, a ordem constitucional ou a lei moral".

visão do BVerfG, elementos da vida humana que não gozem de proteção expressa por outras liberdades constitucionais mas também sejam importantes para a garantia do livre desenvolvimento da personalidade.[35] Ou seja, trata-se de um direito de caráter subsidiário.

Segundo o BVerfG, as expressões do direito geral da personalidade até então desenvolvidas não seriam suficientes para proteger os usuários de sistemas informáticos. Em especial, o direito afetado não é *autodeterminação informacional*, porque não se trata apenas de proteger os dados privados dos usuários.[36] A classificação de dados como privados depende ainda, muitas vezes, do contexto nos quais os dados são descobertos e da relação que tenham com outros dados. Frequentemente, a infiltração do sistema, que nem sempre possibilita a coleta apenas de dados privados e atinge indiscriminadamente todos aqueles armazenados no dispositivo, não permite, de antemão, verificar o significado dos dados para o afetado e quais outras informações podem ser construídas ao relacionar esses dados entre si. Por isso, haveria o risco de formação de perfis da personalidade do indivíduo usuário do sistema. O acesso a esses sistemas pode alcançar dados potencialmente enormes e expressivos, mesmo antes da execução de medidas dirigidas ao levantamento de dados. Portanto, em relação à gravidade que representa para o direito à personalidade do afetado em relação ao levantamento de seus dados individuais, a proteção conferida pelo direito à autodeterminação não seria suficiente para proteger contra todos os riscos da infiltração online.

(2) Diante dessas conclusões, o BVerfG entendeu que o caráter subsidiário do direito geral à personalidade – com sua função de suprir lacunas na proteção ao livre desenvolvimento da personalidade do indivíduo – e a proteção da dignidade humana (Art. 2 Abs. 1 c/c Art. 1 Abs 1 GG) demandariam a direta *garantia da confiabilidade e integridade dos sistemas informáticos*, que as expressões até então derivadas desses direitos ainda não seriam capazes de prover. O Tribunal constrói, assim, um novo direito fundamental, com um âmbito de proteção próprio, para dar

[35] Cf. *Greco* (nota 3), p. 33 e s.

[36] BVerfGE 120, 274 (311 e ss.).

conta de novos setores em que a personalidade tem de poder livremente desenvolver-se e dos novos perigos que ali se põem.

b) O BVerfG também dedica algumas considerações sobre as *intervenções* nesse direito. Haverá uma intervenção caso os órgãos públicos acessem sistemas que, solitariamente ou em razão de conexões técnicas, possam conter dados pessoais do afetado em uma certa dimensão e variedade que revelem partes essenciais da forma de vida de uma pessoa ou uma imagem expressiva de sua personalidade.[37] Não apenas em relação ao uso privado do sistema informático, mas também ao uso comercial, é possível, em regra, a partir do comportamento do usuário, obter informações sobre características pessoais ou preferências. Ainda segundo a Corte, essa proteção do direito fundamental se estenderia também, por exemplo, a telefones móveis ou agendas eletrônicas, que dispõem de uma grande variedade de funções e podem abranger e armazenar dados pessoais de variada natureza. Esse direito protege o interesse do usuário de que os dados criados, processados e armazenados no dispositivo continuem privados. Além disso, o sistema estaria protegido contra a intervenção na sua integridade, afetada caso ele seja acessado de tal modo que seu desempenho, suas funções e seus conteúdos armazenados pudessem ser facilitados à utilização por terceiros. Esse direito protegeria, especialmente, contra intervenções ocultas.

c) Como o direito geral de personalidade não é garantido de forma absoluta, mas permite restrições de forma expressa,[38] o BVerfG se manifesta, por fim, sobre a *justificação* de restrições a esse direito.[39] A garantia de confiabilidade e integridade dos sistemas informáticos pode sofrer intervenções tanto com propósitos preventivos (direito de polícia) quanto repressivos, ou seja, para a persecução de crimes (direito processual penal). Intervenções, como vimos (acima, II.), precisam estar justificadas formal e materialmente. O mais interessante, no entanto, são as exigências constitucionais de proporcionalidade estabelecidas pela Corte para uma eventual norma autorizativa.

---

[37] BVerfGE 120, 274 (313 e ss.).

[38] Cf. a nota 34.

[39] BVerfGE 120, 274 (315 e ss.).

aa) Em primeiro lugar, exigiu-se que, tendo em vista a gravidade da intervenção no direito fundamental, ela só seria justificável em razão de perigos concretos para bens jurídicos *extremamente importantes* [*überragend wichtig*], que seriam o corpo, a vida, a liberdade e bens da coletividade que digam respeito aos fundamentos ou à subsistência do estado ou aos fundamentos da existência de seres humanos.[40]

bb) A corte também exigiu que esses perigos concretos estivessem *baseados em elementos fáticos*, que houvesse, ao menos, *uma probabilidade suficiente* de que os perigos concretos se realizassem, e que a medida só pudesse ser *autorizada por um juiz* (reserva de jurisdição).[41] No entanto, essas exigências – que visam impedir que a infiltração online se baseie em suspeitas difusas – já são comuns a muitas outras medidas de intervenção, inclusive muito menos graves que a infiltração online.[42]

cc) A conclusão mais importante do BVerfG, pertinente também a outras medidas de intervenção na personalidade, era a de que o *núcleo da esfera privada* [*Kernbereich privater Lebensgestaltung*] fosse protegido por precauções legais suficientes.[43] A Corte não viu aqui a necessidade de impor proibições gerais de levantamento de dados em determinados âmbitos. No entanto, impôs um mecanismo de proteção de dois níveis:[44] ao mesmo tempo que seria necessário, tecnicamente (por meio de softwares ou dispositivos de busca), tentar garantir que dados do núcleo da esfera privada não fossem levantados, caso tais mecanismos não fossem suficientes para impedir o levantamento destes dados, eles deveriam ser excluídos em uma segunda etapa. A ideia central do BVerfG é a de que, para o desenvolvimento livre da personalidade, é importante assegurar aos indivíduos que expressem sentimentos, reflexões, visões de mundo e experiências pessoais sem medo de estar sendo observados por órgãos estatais. Mesmo que o indivíduo tenha praticado crimes e possa ser investigado por eles, há condições mínimas que não lhe podem ser negadas.

---

40 BVerfGE 120, 274 (328).

41 BVerfGE 120, 274 (326, 328 e ss., 331 e ss.).

42 *Bär*, Comentário à decisão BVErfGE 120, 274, in: MMR 2008, p. 325 e ss. (326).

43 BVerfGE 120, 274 (335 e ss.).

44 *Bär*, MMR 2008, p. 326.

O *núcleo da esfera privada* é um conceito que surge da *teoria das esferas* de Hubmann para o direito civil.[45] Essa ideia pode ser melhor concretizada se imaginarmos três círculos concêntricos. O externo seria o da *esfera social* ou pública, que está sujeita a intervenções sem altos pressupostos de justificação, e é afetado por perguntas sobre a vida social ou pública, como a profissão, ou pequenas pesquisas online sobre o que é público a respeito do investigado. O intermediário seria o da *esfera privada* ou do sigilo, que exige maiores pressupostos de justificação e é afetado por coleta de informações, p.ex., sobre a rotina de uma pessoa, sobre suas compras e seu círculo de amigos. E, por fim, o círculo interno seria o *núcleo da esfera privada*, que não comportaria qualquer intervenção. Trata-se, portanto, do conteúdo essencial do direito à privacidade, sobre o qual falamos anteriormente (acima, II.), e é uma expressão da dignidade humana.[46] O que está contido nesse núcleo é controverso. A princípio, o BVerfG nega que uma informação pertença ao núcleo da vida privada, caso ela tenha alguma relação imediata com crimes. Essa parece ser a única conclusão atualmente alcançável, com certa segurança, a partir dos julgados da Corte. A proteção absoluta de diários já foi objeto de empate no BVerfG em 1989,[47] e o voto "vencedor" (em questão de empate não se declara a inconstitucionalidade) se baseava, principalmente, no fato de que os registros tratavam de crimes e no argumento de que quem faz uso da forma escrita, renuncia a um total controle sobre os conteúdos correspondentes.[48]

Embora essa decisão do BVerfG se refira a norma do direito de polícia, as balizas de legitimaçãoe para uma eventual norma autorizativa também parecem aplicar-se, naquilo que cabível, ao processo penal. O legislador alemão, tentando se orientar por essas diretrizes, autorizou, no Código de Processo Penal alemão (§ 100b StPO), o uso da infiltração online para a persecução de crimes.

---

45 *Greco* (nota 3), p. 34.

46 Cf. *Greco* (nota 3), p. 34.

47 BVerfGE 80, 367.

48 *Greco* (nota 3), p. 72.

IV. Observação intermediária da perspectiva brasileira

O exposto já nos coloca em posição de responder à primeira pergunta formulada no artigo, quanto à legitimidade abstrata da infiltração online, da perspectiva do direito processual penal brasileiro. Se levarmos a sério a ideia de reserva de lei insculpida no art. 5 II CF, basta verificar que inexiste dispositivo expresso que autorize a medida, para concluir que ela é *inadmissível entre nós*.

Seria necessário apenas esclarecer a razão específica pela qual ela precisa ser expressamente prevista, concretamente: *em qual dos direitos previstos no art. 5º CF ela intervém*? Trata-se de intervenção no âmbito de proteção do art. 5º X, que declara "invioláveis a intimidade, a vida privada ... das pessoas", ou do art. 5º XII, que também qualifica de "inviolável o sigilo ... de dados"? Ou há necessidade de recorrer a um novo direito fundamental não-escrito relativo à confiabilidade e integridade dos sistemas informáticos? Tendemos para essa última posição. Ainda que o conteúdo armazenado no computador se refira a aspectos da vida alheios à intimidade ou à vida privada, ou seja, se encontre fora do âmbito do art. 5º X CF, ele nos parece digno de proteção. Além disso, o "sigilo de dados" mencionado no art. 5º XII CF se refere a dados, não à própria máquina, que pode encontrar-se ainda vazia, por assim dizer, em estado virgem. Temos, assim, a impressão de que haja uma necessidade dogmática de recepcionar a figura do direito fundamental à *confiabilidade e integridade dos sistemas informáticos*, extensão a que a própria CF expressamente se abre (art. 5º § 2º CF: "Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados...").

Se quisermos dotar as nossas instâncias persecutórias de uma faculdade de intervir nesse direito, precisaremos, assim, de *lei específica que a fundamente* (e não apenas a regule). Enquanto inexistir essa lei, o acesso ao conteúdo de sistemas informáticos terá de ocorrer através das medidas da busca e da apreensão do dispositivo físico em que esse conteúdo se encontra armazenado. O legislador não estará livre para dotar essa lei do conteúdo que queira, mas terá de atender a exigências constitucionais que, se não necessariamente coincidem com as que acabamos de expor, que o BVerfG formulou para a Alemanha (acima, III.

2.), deveriam ao menos delas tomar conhecimento. Também por isso, parece-nos interessante observar como o legislador processual penal alemão atendeu a essas exigências por meio do novo dispositivo sobre a medida, introduzido em 2017. É a isso que agora nos voltamos.

V. A infiltração online no processo penal da perspectiva do legislador alemão: o novo § 100b StPO

Em julho de 2017, com a intenção de melhorar a efetividade e praticabilidade do processo penal na Alemanha,[49] o legislador inseriu no Código de Processo Penal alemão, dentre outras normas, a do § 100b, que autoriza a infiltração online com base nas exigências estabelecidas, até então, pelo BVerfG. Passemos em rápida revista seus principais pressupostos de aplicação (1.) e os mecanismos legais de proteção do indivíduo durante a execução da medida (2.).

1. Os principais pressupostos autorizadores da infiltração online nos termos do § 100b StPO

a) A suspeita do fato

Em primeiro lugar, a medida só pode ser autorizada diante da suspeita do fato. As normas processuais penais alemãs fazem referência a três tipos de suspeitas, para distintas fases processuais: a suspeita inicial [*Anfangsverdacht*], a suspeita forte [*dringender Verdacht*] e a suspeita suficiente [*hinreichender Verdacht*]. [50] Enquanto a *suspeita forte* é afirmada nos casos em que, segundo o estado atual da investigação, haja grande

[49] Críticos a esse mote da reforma *Schünemann*, Legitimation durch Verfahren?, StraFo 2015, p. 177 e ss. (186 e ss.); *Greco*, Fortgeleiteter Schmerz – Überlegungen zum Verhältnis von Prozessabsprache, Wahrheitsermittlung und Prozessstruktur, in: GA 2016, p. 1 e ss. (14). Para críticas sobre o procedimento legislativo para a introdução da norma no Código de Processo Penal alemão, *Beukelmann*, Online-Durchsuchung und Quellen-TKÜ, NJW-Spezial 2017, 440.

[50] Ver *Greco* (nota 3), p. 59; e *Gleizer*, in: Hilgendorf/Valerius, Direito Penal: Parte Geral, São Paulo, 2018, p. 153, nota de tradutor.

probabilidade de que o imputado tenha praticado o crime, a *suspeita suficiente* é afirmada quando o imputado tem mais chance de, em vista das provas colhidas, ser condenado do que absolvido. Mas isso não significa que esta esteja abrangida por aquela, já que a suspeita suficiente é verificada sempre ao término dos procedimentos investigatórios, enquanto a suspeita forte se baseia no estado atual da investigação, que pode vir a ser alterado. A suspeita inicial corresponde à nossa *notitia criminis*, uma vez que impõe a instauração de uma investigação preliminar; a suspeita suficiente, à nossa justa causa, impondo a propositura da denúncia. A suspeita forte autoriza, principalmente, a prisão preventiva (ao lado de outros pressupostos, como a fuga ou o perigo de fuga).

Em que pese o legislador não ter estabelecido expressamente o nível da suspeita apta a fundamentar a autorização de infiltração online (§ 100b Abs. 1 Nr. 1 StPO: "fatos determinados fundamentem a suspeita"), o BVerfG entende, em relação à escuta ambiental (§ 100c StPO), que a suspeita precisa ser maior do que uma mera suspeita inicial.[51] O BGH[52] parece ser menos exigente: ele afirma a desnecessidade de uma suspeita forte ou suficiente, e contenta-se com o que ele chama de suspeita *simples* [*einfacher Verdacht*], categoria desenvolvida pela jurisprudência, cuja relação com a tripartição tradicional ainda não foi de todo esclarecida.

O que está claro é que não bastam meros boatos, desconfianças e suposições não verificadas; tampouco bastam suposições especulativas, relativas ao pertencimento a um grupo ou mesmo à experiência criminalística dos investigadores, mas sem base no caso concreto. É necessário que, em razão de circunstâncias relacionadas ao caso, a partir de depoimentos de testemunhas, observações ou outros indícios fáticos, haja indicação, em grau significante, do cometimento de um crime do catálogo de fatos, ou seja, é exigida uma *base fática sólida*, apoiada em circunstâncias concretas

---

[51] BVerfGE 109, 279 (350); *Wolter/Greco*, in: *Wolter* (coord.), Systematischer Kommentar zur Strafprozessordnung (= SK-StPO), vol. 2, 5a. ed., Köln, 2016, § 100a nm. 43.

[52] BGH NStZ 2010, 711; BeckRS 2016, 15673. Nessas decisões, o BGH analisa o grau de suspeita necessário para a medida de monitoramento de telecomunicações (§ 100a StPO).

e de certa extensão.[53] Está claro que a suspeita é sempre uma prognose, a realizar-se no momento da autorização da medida; não é possível, assim, fundamentação retrospectiva, por meio de informações eventualmente obtidas após a autorização da medida.[54]

b) O catálogo de fatos

A medida só pode ser autorizada para a investigação dos crimes previstos no catálogo de fatos da norma autorizativa. Esse pressuposto tem seu fundamento não apenas no princípio da proporcionalidade, que exige a imposição de um rol de crimes especialmente graves, como também na exigência de reserva de lei, no sentido de que a lei tem de fixar os precisos limites da medida.

Ao concretizar o novo direito fundamental à confiabilidade e integridade de sistemas informáticos, o BVerfG estabeleceu, como visto (acima, III. 2. c] aa]), que o emprego da infiltração online só seria justificável em razão de perigos concretos para bens jurídicos *extremamente importantes*, que seriam o corpo, a vida, a liberdade e outros bens importantes para a coletividade, cuja ameaça colocaria em risco as bases ou a existência do estado de direito ou as bases da existência dos seres humanos.[55] Por exigência do BVerfG,[56] o legislador estabeleceu um catálogo de crimes especialmente graves como pressuposto para a infiltração online. Consequentemente, o legislador criou um catálogo único de crimes para a infiltração online (§ 100b Abs. 2 StPO) e para a escuta ambiental (§ 100c Abs. 1 Nr. 1 StPO), medidas mais invasivas à privacidade do que o monitoramento de telecomunicações (§ 100a StPO), cujo catálogo prevê crimes (meramente) graves.

---

[53] BVerfGE 100, 313 (395); BVerfG NStZ 2003, 441 (443); BGH NStZ 2010, 711; *Wolter/Greco*, SK-StPO, § 100a nm. 43; *Graf*, in: Graf (coord.), Beck'scher Online-Kommentar Strafprozessordnung (= BeckOK StPO), 33ª. ed., 1.4.2019, § 100b nm. 12.

[54] *Graf*, BeckOK StPO, § 100b nm. 12, 13.

[55] BVerfGE 120, 274 (328).

[56] BVerfGE 10, 274 (334).

c) A gravidade no caso concreto

Ao criar a norma autorizativa, o legislador ainda se preocupou em positivar um firme posicionamento da jurisprudência constitucional,[57] estabelecendo a necessidade de que a medida esteja baseada não só na gravidade abstrata do crimes, ou seja, no fato dele constar do *catálogo de crimes* especialmente graves, mas também em sua *gravidade concreta* (§ 100b Abs. 1 Nr. 2 StPO: "... o fato é de especial gravidade também no caso concreto"), que deve estar refletida nas específicas circunstâncias em que ele tenha ocorrido.[58] Pode-se dizer que, enquanto a exigência de gravidade abstrata é a concretização da ideia de proporcionalidade que o direito fundamental impõe ao legislador, a exigência de demonstração da gravidade concreta é o seu efeito em relação ao juiz. Como exemplo de gravidade concreta, pode-se mencionar uma grande vantagem em um crime de corrupção ou os efeitos de um crime para a vítima,[59] ou o cometimento de simultâneo de vários fatos integrantes do catálogo,[60] ou o cometimento a partir de uma estrutura organizada.[61]

d) A subsidiariedade

A infiltração online também só pode ser autorizada caso a investigação dos fatos ou do local onde se encontre o afetado, seja, "de outro modo, impossibilitada ou fundamentalmente dificultada" (§ 100b Abs. 1 Nr. 3 StPO). A ideia é afastar a possibilidade de que se lance mão, diretamente, de medidas muitos invasivas quando outras menos invasivas são possíveis. Entre essas medidas encontram-se, principalmente, a busca e a apreensão.[62] A medida pressupõe, assim, um estado de necessidade probatório.[63]

---

[57] BVerfGE 109, 279 (345 e s.).

[58] *Soiné*, NStZ 2018, p. 498 s.

[59] *Graf*, BeckOK StPO, § 100b nm. 15.

[60] *Bruns*, in: Hannich (coord.), Karlsruher Kommentar zur Strafprozessordnung, 8a. ed., München, 2019 (= KK-StPO), § 100b nm. 8.

[61] *Bruns*, KK-StPO, § 100b nm. 8.

[62] Cf. a fundamentação oficial da lei, Bundestag-Drucksache 18/12785, p. 55; *Bruns*, KK-StPO, § 100b nm. 9.

[63] Sobre esse conceito *Greco* (nota 3), p. 61.

Em síntese, costuma-se afirmar que outras medidas *impossibilitam* a investigação [a tornam *aussichtlos*], caso não existam outros meios de encontrar a informação pretendida ou os meios existentes não apresentem perspectiva de mesmo resultado qualitativo. Já o critério de *dificuldade fundamentalmente maior* pode ser afirmado diante de um possível atraso temporal da investigação ou do fato de que medidas alternativas poderiam encontrar apenas informações piores ou não obter as informações adequadas e suficientes para uma investigação mais rápida e eficiente.[64] Altos custos de medidas alternativas também podem justificar a subsidiariedade, desde que eles se mostrem indefensáveis segundo um juízo de proporcionalidade, que leve em conta a gravidade da intervenção.[65] No entanto, deve-se lembrar que a infiltração online também é uma medida de alto custo financeiro.[66]

e) A proporcionalidade em sentido estrito

As considerações de proporcionalidade exigem que não apenas o legislador, mas também o aplicador da lei verifique, antes e durante a execução da medida, se a intervenção é proporcional em relação aos resultados esperados ou à culpabilidade do afetado.[67] Aqui, cabem considerações de muitas ordens, como, por exemplo, a possibilidade de obter muito mais informações não vinculadas ao caso do que o contrário, ou uma grande distância temporal entre a execução do fato e a aplicação da medida, que sugira que o afetado não possua mais as provas do fato em seu dispositivo informático.[68]

f) Os possíveis afetados pela medida

De regra, a medida só pode ser dirigida contra o investigado (§ 100b Abs. 3 S. 1 StPO). No entanto, a medida também pode ser autorizada

---

64 *Graf*, BeckOK StPO, § 100b nm. 16.

65 *Graf*, BeckOK StPO, § 100b nm. 16.

66 *Graf*, BeckOK StPO, § 100b nm. 6.

67 *Graf*, BeckOK StPO, § 100b nm. 20.

68 *Graf*, BeckOK StPO, § 100b nm. 20.

caso seja de se esperar que, inevitavelmente, também venham a ser obtidas informações relacionadas a terceiros não-implicados (§ 100b Abs. 3 S. 2 StPO).[69] Essa é, na realidade, a regra em relação a tais medidas, já que sistemas informáticos contemporâneos dificilmente contêm informações relacionadas apenas ao usuário principal.

Sistemas informáticos de terceiros também podem ser objeto da medida caso sejam utilizados pelo investigado (mesmo sem a anuência do terceiro),[70] mas isso somente se a execução da medida apenas contra o investigado não for suficiente para a elucidação dos fatos ou da localização de um co-investigado.[71] Exemplos de terceiros afetados são familiares, amigos, vizinhos, e mesmo a vítima do crime.[72] Um outro exemplo de sistema informático de terceiros são os espaços de armazenamento em nuvem [*cloud-computing*], que pertencem, em regra, a empresas privadas.[73] A infiltração online de nuvens também levanta questões de cooperação jurídica internacional, tendo em vista que estes sistemas privados estão, em sua maioria, alocados fisicamente em diferentes países.[74]

2. Mecanismos de proteção do indivíduo durante a execução da infiltração online

Além dos pressupostos estabelecidos para a execução da medida, o legislador alemão também estabeleceu regras para a proteção do indivíduo durante a execução da infiltração online no processo penal.

---

[69] Sobre as diversas categorias de terceiros no processo penal alemão *Greco* (nota 3), p 62.

[70] *Graf*, BeckOK StPO, § 100b nm. 23; *Blechschmitt*, Quellen-TKÜ und Online--Durchsuchung, StraFo 2017, p. 361 e ss. (364); *Soiné*, Die strafprozessuale Online-Durchsuchung, NStZ 2018, p. 497 e ss. (499).

[71] *Graf*, BeckOK StPO, § 100b nm. 23.

[72] *Soiné*, NStZ 2018, 499 (499).

[73] Especificamente sobre o acesso a dados armazenados em nuvens, cf. a monografia de *Grözinger*, Die Überwachung von Cloud-Storage, Baden-Baden, 2018. Cf. também *Soiné,* NStZ 2018, 499 (500).

[74] Cf., por todos, *Soiné* NStZ 2018, 499 (500), com outras referências.

a) As cautelas técnicas e os protocolos do procedimento

Em razão da intervenção na integridade do sistema informático, são exigidas cautelas técnicas, com a finalidade de reduzir a intervenção ao mínimo possível e impedir o acesso desautorizado de terceiros por meio dos mecanismos utilizados pelo investigador. Desde o início, as manipulações necessárias para a execução da infiltração online devem ser praticadas com mecanismos que desfaçam de forma automática os efeitos da medida tão logo ela deixe de vigorar (§ 100b Abs. 4 StPO c/c § 100a Abs. 5 S 1 Nr. 3 StPO).

Além disso, e mais importante, por razões de proteção de dados, é o dever de tomar todas as precauções técnicas possíveis para impedir alteração, eliminação e conhecimento desautorizado dos dados copiados por parte de terceiros (§ 100b Abs. 4 StPO c/c § 100a Abs. 5 S. 2, 3). Isso significa que o local de armazenamento dos dados copiados, por exemplo, deve ser protegido, por mecanismos de segurança, tanto físicos quanto virtuais, contra acesso, por exemplo, de funcionários da repartição não autorizados à investigação e de particulares.

Para a proteção efetiva do direito fundamental do afetado e da validade das provas obtidas, o legislador ainda exige (§ 100b Abs. 4 StPO c/c § 100a Abs. 6 StPO) o registro de informações como a qualificação do meio técnico utilizado e o momento de sua utilização, a identificação do sistema informático e as alterações realizadas que não sejam simplesmente transitórias, os dados levantados e o departamento que executa a medida. Essas informações têm o condão de possibilitar a posterior verificação da proporcionalidade da medida durante a execução, a forma e a abrangência da intervenção, a obediência aos limites temporais, a tomada de todas as cautelas técnicas, a atribuição de responsabilidade e a qualificação das testemunhas da execução da medida.

Há quem afirme que esse dever de atender a cautelas técnicas fundamente quase que uma posição de garante daqueles que executam a infiltração.[75] Essas considerações concretizam a ideia de que poderes vêm com responsabilidades. Para a proteção efetiva do direito fundamental do afetado e da validade das provas obtidas, o legislador ainda exige o

[75] *Graf*, BeckOK StPO, § 100b nm. 29.

registro de informações relativas à execução da medida, a fim de possibilitar o controle posterior da custódia da prova e da responsabilidade dos agentes envolvidos em sua produção. Esses registros são chamados de protocolos do procedimento.

b) Proteção do núcleo de privacidade

Em relação à proteção dos espaços absolutos da vida do indivíduo (o conteúdo essencial dos direitos fundamentais), o legislador estabeleceu a *inadmissibilidade* da infiltração online (§ 100d Abs. 1 StPO) em situações nas quais se possa supor, com base em elementos fáticos, que a execução da medida venha a obter *apenas* informações do núcleo da esfera privada. O critério *apenas* é merecedor de muitas críticas da ciência.[76] Afirmam alguns, entre os quais o primeiro autor do presente que artigo, que seria praticamente impossível concluir a priori que outras informações, não pertencentes ao núcleo da esfera privada, não possam ser também obtidas mesmo nos mais íntimos espaços do indivíduo, essa regra não teria qualquer aptidão para proteger aquilo que justamente deve ser objeto de máxima proteção. A lógica deveria ser inversa. A legislação deveria proibir a execução da medida, caso, segundo elementos fáticos, sua execução ameaçasse a obtenção *também* de informações do núcleo da esfera privada, ainda que outras pertinentes ao caso pudessem ser obtidas. Essa ideia já foi concretizada pelo BVerfG em relação ao monitoramento de e-mails, quando a Corte, por interpretação redutiva conforme à constituição, vedou o acesso a telecomunicações caso algum conteúdo do núcleo da esfera privadas pudesse ser alcançado.[77]

Especificamente em relação à infiltração online, criou-se também a exigência de que, desde que possível, se assegure, com meios técnicos, que não sejam obtidos dados do núcleo da esfera privada (§ 100d Abs. 3 StPO). E que, na ocasião em que tais dados, apesar das precauções técnicas tomadas, porventura venham a ser obtidos, eles devem ser imediatamente eliminados ou submetidos ao juízo para apreciação sobre a possibilidade

---

[76] Cf., com outras referências, *Wolter/Greco*, SK-StPO, § 100a nm. 57 e ss..

[77] BVerfGE 124, 43 (69 s.). Cf. também *Wolter/Greco*, SK-StPO, § 100a nm. 57, com outras referências.

de serem valorados ou a necessidade de serem eliminados. Diferente de outras precauções, estabelecidas conjuntamente para o monitoramento de telecomunicações, a escuta ambiental e a infiltração online, aqui o legislador cria uma precaução aplicável apenas a esta última. Isso pode indicar que, em sua visão, diferente das demais medidas, a infiltração online permite alguma distinção prévia da natureza das informações por não servir à vigilância concomitante das atividades do investigado em seus sistemas informáticos, senão apenas à busca por arquivos já armazenados (abaixo, IV.).

c) Proteção dos portadores de um direito de recusa a testemunhar

Em relação à proteção do direito a não testemunhar contra o investigado (§ 100d Abs. 5 S. 1 StPO), a infiltração online é inadmissível para a produção de provas relacionadas a pessoas autorizadas a negar testemunho contra o investigado em razão da *profissão* (§ 53 StPO). Se, durante ou após a execução das medidas, passar a existir uma situação que autoriza a recusa a testemunhar, as informações obtidas não apenas não poderão ser valoradas, como deverão ser eliminadas imediatamente; nesse caso, a obtenção das informações e sua eliminação deverão ser documentadas (§ 100d Abs. 5 S. 2 c/c § 100d Abs. 2, S. 2 e 3 StPO). Em relação a pessoas autorizadas a negar testemunho em razão de *parentesco* (§ 52 StPO), as informações obtidas por meio da infiltração online só podem ser valoradas, caso o significado da relação de confiança não seja desproporcional ao interesse na investigação dos fatos ou da localização de um investigado (§ 100d Abs. 5 S. 2 StPO).

O direito de negar testemunho enquanto direito fundamental processual é entendido como consequência da ideia de proteção dos direitos fundamentais. Portanto, o legislador também estabeleceu proteção aos portadores desse direito, não permitindo que a infiltração online o viole. O que se pretende com essas regras é evitar a circunvenção do direito de não testemunhar contra o investigado, ou seja, que, diante da impossibilidade de se obrigar alguém a testemunhar, se permita obter as informações, por via transversa, de maneira oculta. Os advogados de defesa do investigado, diferente de todas as outras pessoas autorizadas a negar

testemunho, gozam do que se chama de *dupla proteção*.[78] As informações que eles trocam com o investigado não podem ser obtidas, em primeiro lugar, por uma garantia individual de que este não seja degradado a objeto do processo, mas também pela proteção público-institucional da relação de confiança essencial para o processo.

d) A proteção dos dados coletados: os imperativos de identificação, de notificação e de eliminação

Por fim, em razão da necessidade de proteção dos dados pessoais obtidos por meio de intervenção na esfera de privacidade do investigado, o legislador também estabeleceu uma série de cautelas adicionais, que valem para todas as medidas secretas.

Em primeiro lugar, os dados pessoais obtidos com a execução da medida devem ser *identificados* como tais, e se forem transferidos a outra instituição do Estado, a estas caberá manter a identificação (§ 101 Abs. 3 StPO).

Além disso, a fim de permitir àquele que teve o próprio âmbito de proteção afetado que submeta a medida a um controle judicial posterior, a lei também cria o dever de que o Estado, em regra, o *notifique* sobre a afetação (§ 101 Abs. 4 StPO). Essa regra é excepcionada em razão de interesses preponderantes de um terceiro (Abs. 4 S. 3). O imperativo de notificação surge no momento em que não houver riscos aos propósitos da investigação, à vida, à integridade física e à liberdade pessoal de uma pessoa; e o atraso da notificação superior a seis meses a partir do encerramento da medida é carente de autorização judicial (Abs. 6 S. 5).

Por fim, quando dados pessoais obtidos não forem mais necessários para a persecução penal ou para um eventual controle judicial da medida, eles devem ser imediatamente *eliminados* (§ 100d Abs. 8 StPO). A eliminação deve ser certificada nos autos (Abs. 8 S. 2) e, caso os dados sejam mantidos apenas para uma eventual verificação judicial da medida, eles não podem ser utilizados para nenhum outro propósito sem o consentimento do afetado, devendo ser acautelados de forma apropriada (Abs. 8 S. 3). O imperativo de eliminação dos dados tem por finalidade

[78] *Wolter/Greco*, SK-StPO, § 100a nm. 56.

reduzir a possibilidade de acesso a informações pessoais não (ou não mais) necessárias para a prova processual, zelando pela manutenção da proporcionalidade da medida de infiltração online.

VI. Questões especiais da infiltração online

Além dos ordinários problemas interventivos da infiltração em sistemas informáticos e da busca por informações relevantes para um processo penal, ainda há três outras questões que, em nosso entender, também merecem atenção.

1. A vigilância online

Alguns dispositivos informáticos presentes em nosso dia a dia possibilitam, tecnicamente, mais do que uma simples descoberta de informações armazenadas em suas memórias. O acesso remoto a celulares (ou até a uma Smart-TV)[79] permite, por exemplo, a observação simultânea de fatos contemporâneos, por meio da ativação de seus sistemas sensoriais, como microfone e câmera, sem o conhecimento do usuário afetado (vigilância online).[80] Como os celulares são objetos que nos acompanham de perto, do banheiro à beirada da cama, o acesso a esses dispositivos permite não apenas o encontro de informações armazenadas, por exemplo, na caixa de e-mails ou em conversa privada em um aplicativo de mensagens instantâneas, como também acesso ao áudio e vídeo de uma relação sexual, de uma discussão íntima e do diálogo com o médico ou com o advogado de defesa. Por meio de uma vigilância online é possível comprometer não apenas a proteção eficiente do núcleo da esfera privada, como também a própria confiança no uso de dispositivos informáticos, que se transformam em objetos de escuta e gravação ambiental.

Parece-nos que a medida não encontra fundamento legal no direito alemão, de modo que ela é impossível de *lege lata*. Isso vale com

---

[79] *Záboji*, „Unheimliche Bilder“, in: Frankfurter Allgemeine Zeitung, publicado em 8.6.2016, acessível em: http://bit.ly/2LZUCKM.

[80] Cf. *Soiné* NStZ 2018, 499 (502).

ainda maior razão para o Brasil. *Não se trata de uma infiltração online*, nos termos do § 100b StPO. A medida legalmente prevista permite um acesso à memória do dispositivo infiltrado, de forma que dele se extraiam informações já ali contidas. A vigilância online transforma o aparelho em câmera ou escuta, que produz novas informações.

Esse caráter produtivo da medida a aproxima da *vigilância acústica domiciliar*, autorizada, na Alemanha, pelo § 100c StPO, e mencionada no Brasil pelo art. 3º II Lei 12.850/2013 para investigação de organizações criminosas.[81] Parece-nos, entretanto, que *tampouco* esses dispositivos dão conta da medida. A vigilância acústica domiciliar distingue-se da vigilância online pelo fato de esta, em virtude da maior confiança que conferimos a nossos dispositivos pessoais, ampliar nossa exposição e vulnerabilidade e, além disso, utilizar-se de meios técnicos que nos pertencem, manipulando-os e, com isso, afetando também a integridade dos dispositivos informáticos privados. Os sistemas informáticos utilizados para uma vigilância online não são meios técnicos à disposição e de propriedade dos órgãos de persecução penal, mas dos afetados pela medida. Se trouxermos para casa um mero utensílio doméstico, como uma televisão com acesso à internet, estaremos, em última instância, trazendo um espião ao lar. Por se tratar de uma intervenção de qualidade distinta, seria necessário que estivesse autorizada expressamente como forma de execução da escuta ambiental.[82]

2. Métodos técnicos de infiltração online e problemas

Além da infiltração ordinária – com superação técnica dos obstáculos de segurança do dispositivo informático, por exemplo, por meio da obtenção das senhas do sistema – há, a princípio, outras três possibilidades técnicas de infiltração a dispositivos informáticos: por meio de a) acesso físico ao dispositivo para a instalação de malwares, b) colaboração

---

[81] Ocorre que a medida é ali apenas mencionada; não há dispositivo que a preveja em seus pressupostos, de forma que, a nosso ver, falta uma base legal também para essa medida no direito brasileiro, cf. já *Greco* (nota 3), p. 40.

[82] Cf. *Rüscher*, Alexa, Siri und Google als digitale Spione im Auftrag der Ermittlungsbehörden?, NStZ 2018, p. 687 e ss.

do afetado para a instalação de malwares no seu próprio dispositivo e c) lacunas de segurança existentes em algum software do dispositivo. Cada um desses três métodos levanta diferentes questões jurídicas, havendo quem os considere de todo ilegítimos.[83]

3. Inconstitucionalidade do § 100b StPO?

Como já demos notícia (acima, III.1.), a constitucionalidade da norma autorizativa para a infiltração online como medida de investigação no processo penal (§ 100b StPO) está atualmente submetida, por reclamação constitucional, à avaliação do BVerfG. Por razões de espaço, nós não discutiremos cada uma das alegadas inconstitucionalidades, mas nos limitaremos apenas a noticiar, dentre todas, três que entendemos mais importantes.[84]

Em primeiro lugar, a constitucionalidade da infiltração online é questionada em razão da amplitude do catálogo de fatos. Em sua decisão de 2008,[85] o BVerfG estabeleceu que o emprego da infiltração online só seria justificável em razão de perigos concretos para bens jurídicos *extremamente importantes*, que seriam o corpo, a vida, a liberdade e outros bens importantes para a coletividade, cuja ameaça colocaria em risco as bases ou a subsistência do estado de direito ou as bases da existência dos seres humanos. Do extenso catálogo de fatos constam, no entanto, crimes que, na visão dos reclamantes, não protegem tais bens jurídicos: entre outros, a falsificação de moeda, a lavagem de dinheiro, a corrupção e a receptação.

---

[83] Nesse sentido *Derin/Golla*, Der Staat als Manipulant und Saboteur der IT-Sicherheit, in: NJW 2019, 1111 ss. (1112 ss.). Ver também, com outra posição, *Soiné* NStZ 2018, 499 (500 ss.); *Bruns*, KK-StPO, § 100b nm. 6.

[84] Para as demais, cf. a síntese da Reclamação Constitucional, no site do partido político *Freie Demokratische Partei* (FDP) ajuizador da ação, em: https://www.fdp.de/sites/default/files/uploads/2018/08/20/fdp-vfb-gazeas-zusammenfassung.pdf. Conferir, também, a entrevista com o advogado do Reclamante, Nikolaos Gazeas, em: https://www.lto.de/recht/hintergruende/h/verfassungsbeschwerde-staatstrojaner-fdp-anwalt-interview-online-durchsuchung/.

[85] BVerfGE 120, 274.

Outra alegação de inconstitucionalidade se refere a uma proteção ineficiente do núcleo da esfera privada. Além do fato de a norma não prever uma proibição absoluta de levantamento de determinados dados, limitando-se a simplesmente proibir uma ulterior valoração dos mesmos (§ 100d Abs. 2 StPO), o legislador também não teria estabelecido a necessidade de que o magistrado fizesse juízo sobre o pertencimento ou não de uma informação ao núcleo da esfera privada antes que os órgãos de persecução penal tivessem acesso a ela.

Por fim, também se aponta inconstitucionalidade na desproporcional ausência de norma que garanta a mesma proteção dos profissionais dispensados do testemunho aos seus auxiliares, de forma que não se possa, por via transversa – acessando, por exemplo, os dispositivos informáticos da secretária do advogado –, esvaziar as garantias do sigilo profissional.

VII. Conclusão

Em síntese, podemos dizer que a infiltração online, como meio processual-penal de obtenção oculta e remota de provas armazenadas em sistemas informáticos é uma medida cada vez mais atraente na era da digitalização, em que informações necessárias ao processo estão, muitas vezes, apenas registradas em formato de dígitos 0-1, e não mais em papéis apreensíveis por meio de medidas convencionais, como a busca e apreensão. Em ordenamentos jurídicos que conhecem direitos fundamentais, ela é, no entanto, certamente uma intervenção. Em qual(is) direito(s) fundamental(is) ela intervém é a primeira pergunta a ser respondida. A resposta a essa pergunta pode nos levar, como na experiência alemã, a reconhecer a necessidade um específico direito fundamental que proteja os indivíduos dos riscos que a vida cercada de dispositivos informáticos pode lhes criar. A concretização de um direito à integridade e confiabilidade no uso de dispositivos informáticos parece ser uma boa resposta, dada pelo BVerfG, ao problema: um direito que proteja não apenas contra invasões à privacidade, mas também contra manipulações em sistemas informáticos privados, de modo que os indivíduos possam confiar em seu uso e, assim, desenvolver livremente suas personalidades na era da digitalização.

Um direito fundamental à integridade e confiabilidade no uso de sistemas informáticos deve criar altos obstáculos interventivos, tendo em vista as sérias consequências que uma intervenção pode criar para a vida dos indivíduos que tenham seus sistemas informáticos acessados por terceiros, especialmente agentes estatais. Esses pressupostos estão sendo discutidos há algum tempo pela ciência e pelos tribunais alemães e podem servir de parâmetro para a elaboração de uma norma autorizativa ainda inexistente no direito brasileiro. Na ausência de norma autorizativa para a infiltração online no ordenamento jurídico brasileiro, a ilegitimidade da medida é evidente. O Estado só pode atuar nos limites das autorizações do povo, conferidas por seus representantes no parlamento.

Como essa autorização inexiste no Brasil, é vedado às instâncias de persecução infiltrar-se em computadores de forma oculta. No Brasil, o acesso ao conteúdo de sistemas informáticos tem de fazer uso da busca e da apreensão do dispositivo físico em que esse conteúdo se encontra armazenado.

Apêndice:

§ 100b Infiltração online:

(1) Sem o conhecimento do afetado [ocultamente], pode-se, com meios técnicos, intervir em seu sistema informático e levantar dados que ali se encontrem, caso

1. fatos concretos fundamentem a suspeita de que alguém consumou ou, caso a tentativa seja punida, tentou consumar como autor ou partícipe, um crime especialmente grave, listado no rol da Abs. 2.,

2. o crime seja especialmente grave também no caso concreto

3. a investigação dos fatos ou do local onde se encontra o acusado, fosse, de outro modo, consideravelmente mais difícil ou infrutífera.

(2) Crimes especialmente graves no sentido da Abs. 1 Nr. 1 são:

1. do Código Penal:

a) crimes de alta traição e de perigo para o estado de democrático de direito... b) constituição de organizações criminosas ... e terroristas ... c) falsificação de moedas ... d) crimes sexuais ... e) pornografia infantil... f) homicídio e homicídio qualificado... g) crimes contra a liberdade pessoal (tráfico de pessoas... prostituição compulsória... escravidão... h) furto em bando... i) roubo grave e roubo com resultado morte... j) extorsão... k) crimes de receptação... l) casos especialmente graves de lavagem de dinheiro, ocultação de valores patrimoniais auferidos ilicitamente... m) casos especialmente graves de corrupção com ou sem infração de dever...

2. da lei de asilo: (...) a...b...

3. da lei de domicílio: a...b...

4. da lei de drogas: a...b...

5. da lei de controle de armas de guerra: a...b...

6. do código penal internacional:

a) genocídio ... b) crimes contra a humanidade c) crimes de guerra d) crimes de agressão

7. da lei de armas: a...b...

(3) A medida só pode se dirigir contra o afetado. Uma intervenção em sistemas informáticos de outras pessoas só é permitida, caso, em razão de fatos concretos, se possa assumir que

1. o afetado mencionado na decisão utilize sistemas informáticos da outra pessoa, e
2. a realização da intervenção apenas nos sistemas informáticos do afetado não possibilite a investigação dos fatos ou do local onde se encontra um co-investigado.
A medida também pode ser executada caso outras pessoas sejam afetadas de forma mediata.

(4) § 100a Absatz 5 e 6 se aplicam, com a exceção da Abs. 5 Satz 1 Nr. 1, naquilo que couber.

§ 100a Abs. 5 e 6:

(5) Em relação à medida, deve-se assegurar tecnicamente que
(...)
2. só sejam realizadas alterações no sistema informático que sejam indispensáveis para o levantamento dos dados, e
3. as alterações realizadas, desde que tecnicamente possíveis, sejam automaticamente excluídas ao término da medida.
O meio empregado deve ser protegido contra utilização desautorizada segundo o estágio da tecnologia. Dados copiados devem, segundo o estágio da tecnologia, ser protegidos contra alteração, exclusão e tomada de conhecimento desautorizados.

(6) Em toda ocasião em que se empregue a medida, é imperativo o registro
1. da qualificação do meio técnico utilizado e do momento de sua utilização,
2. de informações para a identificação do sistema informático e das alterações realizadas que não sejam simplesmente transitórias,
3. de informações que possibilitem a determinação dos dados levantados, e
4. do departamento que executa a medida.

§ 100d StPO:
(1) As medidas dos §§ 100a a 100c são inadmissíveis caso seja possível assumir, com base em elementos fáticos, que suas execuções venham a obter apenas informações relativas ao núcleo da esfera privada.

(2) Informações do núcleo da esfera privada, obtidas por meio das medidas dos §§ 100a a 100c, não podem ser valoradas no processo. Registros de tais informações devem ser imediatamente eliminados. O fato de terem sido obtidas e eliminadas deve ser documentado.
(3) Em relação à medida do § 100b [Infiltração online], deve-se, desde que possível, garantir que dados relativos ao núcleo da esfera privada não sejam obtidos. Informações relativas ao núcleo da esfera privada, obtidas por meio da medida do § 100b, devem ser imediatamente eliminadas ou submetidas, pela promotoria, ao juízo, para decisão a respeito da possibilidade de valoração e da eliminação dos dados. A decisão do juízo a respeito da possibilidade de valoração é vinculante para o outro processo.
(4) ... em relação à medida do § 100c.
§ 101 – Regras procedimentais relativas a medidas ocultas
... (8) Os dados pessoais, obtidos por meio das medidas, que não sejam mais necessários para a persecução penal ou para uma eventual verificação judicial devem ser eliminados imediatamente. Desde que os dados sejam mantidos apenas para uma eventual verificação judicial, eles podem ser utilizados sem o consentimento do afetado apenas para esse propósito; eles devem ser bloqueados.

Referências bibliográficas

Bär, Comentário à decisao BVErfGE 120, 274, in: MMR 2008, p. 325 e ss.

Beukelmann, Online-Durchsuchung und Quellen-TKÜ, NJW-Spezial 2017, p. 440.

Blechschmitt, Quellen-TKÜ und Online-Durchsuchung, StraFo 2017, p. 361

Bruns, in: Hannich (coord.), Karlsruher Kommentar zur Strafprozessordnung, 8a. ed., München, 2019 (= KK-StPO).

Derin/Golla, Der Staat als Manipulant und Saboteur der IT-Sicherheit, in: NJW 2019, p. 1111.

Dimoulis/Martins, Teoria Geral dos Direitos Fundamentais, 5ª. ed., 2014.

Ferreira Mendes/Gonet Branco, Curso de Direito Constitucional, 12ª. ed., 2017.

Graf (coord.), Beck'scher Online-Kommentar Strafprozessordnung (= BeckOK StPO), 33ª. ed., 1.4.2019.

Greco, Fortgeleiteter Schmerz – Überlegungen zum Verhältnis von Prozessabsprache, Wahrheitsermittlung und Prozessstruktur, in: GA 2016, p. 1.

Grözinger, Die Überwachung von Cloud-Storage, Baden-Baden, 2018.

Hilgendorf/Valerius, Direito Penal: Parte Geral, São Paulo, 2018.

Rüscher, Alexa, Siri und Google als digitale Spione im Auftrag der Ermittlungsbehörden?, NStZ 2018, p. 687.

Sarlet, Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988, 10ª. ed. Porto Alegre, 2015.

Sarlet, Teoria geral dos direitos fundamentais, in: Sarlet/Marinoni/Mitidiero, Curso de direito constitucional, 7ª. ed., 2018.

Schünemann, Legitimation durch Verfahren?, StraFo 2015, p. 177.

Soiné, Die strafprozessuale Online-Durchsuchung, NStZ 2018, p. 497 e ss.

Wolter (coord.), Systematischer Kommentar zur Strafprozessordnung (= SK-StPO), vol. 2, 5a. ed., Köln, 2016.

Wolter, O inviolável e o intocável no direito processual penal: reflexões sobre a dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal, São Paulo, 2018.

Záboji, „Unheimliche Bilder", in: Frankfurter Allgemeine Zeitung, publicado em 8.6.2016, acessível em: http://bit.ly/2LZUCKM.

Informações adicionais e declarações dos autores
(integridade científica)

Declaração de conflito de interesses (conflict of interest declaration): os autores confirmam que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

- *Luís Greco*: projeto e esboço inicial, coleta e análise de dados, levantamento bibliográfico, revisão bibliográfica, redação, revisão crítica com contribuições substanciais, aprovação da versão final.
- *Orlandino Gleizer*: projeto e esboço inicial, coleta e análise de dados, levantamento bibliográfico, revisão bibliográfica, redação, revisão crítica com contribuições substanciais, aprovação da versão final.

Declaração de ineditismo e originalidade (declaration of originality): os autores asseguram que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atestam que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 30/07/2019
- Retorno rodada de correções: 16/09/2019
- *Autores convidados*

http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies - custom-1

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editoras-associadas: 2 (BC e CC)

COMO CITAR ESTE ARTIGO:

GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.278

An introduction to AI and criminal justice in Europe

Introdução à inteligência artificial e à justiça criminal na Europa

Serena Quattrocolo[1]
University of Eastern Piedmont – Italy
serena.quattrocolo@uniupo.it
https://orcid.org/0000-0002-6746-1130

Abstract: The article focuses on the need to start a comprehensive and multidisciplinary discussion about the specific interaction between AI and criminal justice, especially within the European context. Indeed, criminal law is considered, for several reasons, a realm in which computational modelling and AI cannot have a direct and relevant application. On the contrary, there is an urgent need to start a legal reflection about both the short- and long-term effects of such technology, that is reshaping all aspects of our social existence, justice included. The purpose of this article is to point out the most relevant risks in this scenario. There is no ambition to deliver answers but, rather, the need to set specific questions about if and how AI can be integrated into the criminal justice European systems. The author delays to a more comprehensive study any attempt of answering such questions.

Keywords: computational models; algorithms; decision-making process; *stare decisis*; judicial independence.

Resumo: *O presente artigo analisa a necessidade de iniciar uma discussão global e multidisciplinar em relação à interseção existente entre a inteligência artificial e a justiça penal, especialmente no contexto europeu. De fato, por diferentes razões, o direito penal é considerado o campo no qual a estrutura computacional e a inteligência artificial não podem obter uma aplicação direta e relevante. Ao contrário, constata-se uma urgente necessidade de iniciar uma reflexão global sobre os efeitos em curto e longo prazo de tal tecnologia, que está remodelando todos os aspectos de nossa existência social, a começar pela justiça. Nesse*

[1] Full Professor of Criminal Procedure.

cenário delineado, o objetivo deste trabalho é evidenciar os riscos mais relevantes atualmente existentes. Contudo, não há a ambição de fornecer respostas, mas, ao contrário, expor perguntas específicas sobre se e como a inteligência artificial possa ser integrada nos sistemas europeus de justiça penal. Remete-se a um estudo mais completo para qualquer tentativa de responder a tais questionamentos.

Palavras-chave: *modelos computacionais; algoritmos; processo decisório; stare decisis; independência judiciária.*

1. Criminal law and the digital revolution

In the common sense, 'criminal law' and 'technology' are considered, traditionally, non-reconcilable terms. Being the ultimate reaction of a jurisdiction to the aggression upon the core values of the society, criminal law is strictly embedded in the social culture. The topic has been dwelled abundantly in the European continental literature, from which we derive the idea that criminal law grasps national *Kulturnomen*, reproducing the general – or, at least, the most common – values of a population.[2] In so far, Criminal Law tends to be, all over the world, a slow-changing factor, clearly because cultural shifts are slow-evolving phenomena: only settled down transformations can be ratified by the law, not only in the statutory-law legal systems.

Although law is one of the means to influence people's behaviour,[3] in democratic societies Criminal Law seems to be unfitted to drive

[2] Cadoppi Alberto, *Il valore del precedente nel diritto penale*. 2nd ed., Giappichelli, Torino, 2014, p. 22.

[3] See Julia Black's perspective on decentred regulation, in which aw is one out of many different systems to influence social behaviour: Black Julia, *Critical*

normative changes in social behaviour, rather to crystallise accomplished processes into sets of commands, reflecting an accepted framework of social values. Indeed, this is perfectly understandable: the harshness of penalties implies that the reject of a specific conduct is shared by a vast majority of the community, as much as the abolition of an offence (either statutory or judge-made) implies a general recognition of legitimacy in such conduct. If not, the legislator is imposing, non-democratically, values and rules that do not reflect common opinions and feelings. In continental criminal law this may indirectly impinge on one of the modern understandings of the rule of law, it is to say 'requirability' (esigibilità), that implies full understanding of the criminal behaviour and command by individuals: the latter could not be expected to avoid criminal behaviours if it is not possible for them to fully and properly grasp what the law considers to be criminal.

However, it is undisputed that, in the last decades, the contemporary society witnessed a computational turn, that, now we all understand,[4] is not only a breath-taking scientific advancement, a radical change in every professional realm, but, overall, is one of the most rapid, astonishing and wide-spread cultural changes ever occurred.[5] This has been touching the foundations of our society[6] in such a way to permeate even the steady core of criminal law.

These preliminary remarks suggest two very general observations. Firstly, if criminal law is a sort of picture of the existing cultural context in a jurisdiction, there is no possibility for it to move ahead, or keep in track with, scientific progress, that is reshaping social habits. Scientific progress will always precede changes and amendments in criminal law.

Reflections on Regulation, in *Australian journal of legal Philosophy,* 2002, vol. 27, 1-36, p. 4

4 Even though some had clearly foreseen it, decades ago: Negroponte Nicholas, *Being Digital*, Hodder&Stoughton, London 1995; Kurzweil Ray, *The Singularity is Near*, Viking, New York, 2005, p. 7, 8.

5 Floridi Luciano, *The Fourth Revolution*, OUP, Oxfrod 2017, passim.

6 See Garapon Antoine, Lassègue Jean, *Justice digitale*, PUF, Paris, 2018, especially 83 ff.: «la revolution numérique bouleverse tous les compartiments de l'existence collective».

Secondly, the impact of the computational turn upon the realm of criminal justice turned out to be much wider than the area of 'traditional' cybercrime. Although the concept of cybercrime acknowledged at the beginning of this Century, as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks"[7], may not be considered wrong in itself, the phenomenon proved much more articulated and sophisticated over the decades. Today, the legal research in that branch of criminal law evolved into an attempt to theorise the application of the classic legal categories to artificial intelligence entities.[8]

Moreover, the digital revolution that globally occurred especially over the last decade is having repercussions upon every aspect of the administration of criminal justice, far behind the aspects that have been addressed by the Budapest Convention on Cybercrime. The turn into a digital society is determining substantial changes not only in the context in which crime may occur, or in the way investigations can be carried on. Delivering justice is a human task and the sudden digital change into individuals' life-style is affecting the way in which such task is performed,[9]

---

[7] See, among the first attempts to define the concept, Sieber Ulrich, *Computerkriminalitaet und Strafrecht*, Carl Haymanns Verlag, Koeln, 1977, passim. Thomas, Loader, p. 3. Although both research and legislation evolved significantly, it is still impossible to give one, unique and undisputed definition of cybercrime. "Cybercrime is a container term of convenience, describing a collection of acts or a field of criminal activity, rather than a single concept": Boister Nicholas, *An introduction to Transnational Criminal Law*, 2nd ed., OUP 2018, 188. Moreover, many other similar terms are often used, such as 'computer crime','IT crime'... It has been said that the concept encompasses a whole range of terms which imply that the digital technology (not only computers) is an element of the offence. In this sense, internet connections are necessary elements, either for crimes against digital technologies and crime committed by means of digital technologies: Sieber Ulrich, *Mastering Complexity in the Global Cyberspace: the Harmonisation of Computer-Related Criminal Law*, in M. Delmas Marty, M. Pieth, U. Sieber (eds), *Les Chemins de l'harmonisation pénale*, 2008, 127

[8] Pagallo Ugo, Quattrocolo Serena, *The Impact of AI on Criminal Law and its twofold procedures*, in W. Barfield, U. Pagallo, *Research Handbook on the Law of Artificial Intelligence*, 2018, Edgar Elgar, p. 400

[9] See the seminal work of Susskind Richard, *The End of Lawyers?*, OUP, 2008.

impinging on the inner aspects of it, such as the decision-making process. These aspects will be analysed in the following paragraphs.

What has been briefly observed here can be considered the cause of an undisputed trend. If regulation in the criminal area tends to follow (not to precede) social changes, the digital turn occurred out of (and before) a specific legal framework. This implies that the digital advancement has been taking place in the absence of a back-ground research on the risks it may entail to the area of the core values of the society, usually protected by criminal law. Moreover, for a long time, the development of digital solutions overlooked the specific needs of criminal justice: existing (and pre-existing) technology dripped onto (almost every) criminal justice systems, providing availability of methods and solutions having been tailored for different purposes and not expressly fitted for the judicial use.

In particular, the computational revolution meant availability of enormous quantity of free data, constantly generated by digital devices, powerful computational resources, being able to mine uncountable amounts of data in few seconds and ever cheaper storage costs.[10] Such conditions (quintillions of data and cheap, unprecedented computational power) set the premises for offering, also to the criminal justice systems, useful facilities, even though not specifically tailored for the task.[11] The digital turn provided not only full ranges of data, that can be used as evidence in criminal proceedings, but also new investigation systems, based on mining and analysing huge sets of available data (private or not; personal or not). Not only full digitalisation of courts' decisions, with unrestricted access to any case-law, but also more or less sophisticated software for the analysis of it, to find patterns of predictability within judicial decisions. Moreover, the availability of an unprecedented amount of digital data shifted the attention from a code-based modelling system (code-driven regulation),[12] totally deterministic - in which the discretion

[10] Katz Daniel M., *Quantitative Legal Prediction, Or- How I Learned to Stop Worrying and Start Preparing for the Data-Driven Future of the Legal Services Industry*, in *Emory Law Journal*, 2013, 909-966, p. 916.

[11] Floridi Luciano, cit., 41.

[12] For the distinction between code-driven and data-driven regulation, see Hildebrandt Mireille, *Algorithmic Regulation and the Rule of Law*, *Philosophical*

is encrypted in the expert-designed code, establishing that If This, Than That – to a deep-learning modelling system, non-deterministic, in which the discretion lays in the choice of the data set (data-driven regulation) of legal texts to be used to train the system.[13]

All this happened without a proper and effective confrontation between computer scientists, leading the sensational digital revolution, and criminal law experts. Also the legal literature confirms this impression, testifying of a growing attitude, especially in the U.S., of private law to focus on the theoretical challenges inherent the application of automation and artificial intelligence to the everyday-life, since Lawrence Solum's seminal article in 1992,[14] accompanied by a slower trend in criminal law, and in criminal procedure.[15] To some extent, this matches with the premises from which I moved, it is to say, the connate feature of criminal law to following rather than preceding (or progressing with) social changes...[16]

2. Realism v. dystopianism

It Is essential, for the goal of this work, to understand how much of the mistrust and fears of (European) criminal lawyers towards the most recent digital instruments is due to the fact that they (allegedly) bring automated decision making processes into criminal justice or, rather, that

Transactions of the Royal Society, 2018, p. 2, 3.

[13] There is no room here for reconstructing the evolution of AI applied to legal issues. For a general overview, See Rissland Edwina, Ashley Kevin D., Loui R.P., *AI and Law: A fruitful synergy*, *in Artificial Intelligence,* 2003, Special Issue, 2.

[14] Solum Lawrence, *Legal Personhood for artificial intelligences*, in *North Carolina Law Review*, 1992, p. 1231-1288

[15] Nieva Fenoll Jordi, *Inteligencia artificial y proceso judicial*, Marcial Pons, Madrid, 2018, 33 ff.

[16] This attitude has been recently studied under the sociological point of view: see Christin Angèle, *Algorithms in practice: Comparing web-journalism and criminal justice,* in *Big Data and Society*, 2017 (July-December), p. 1-14. Based on his empirical research in American local criminal courts, the author concludes that "in criminal justice innovation does not come with the glitter and appeal that it has in other sectors: it is often a source of uncertainty, as innovation arrives without the vetting of precedent".

they bring algorithmic decision making-processes into it. Let's clarify this statement, that may sound slightly tautologic.

2.1. The complexity of algorithmic decisions

According to a quite common definition,[17] "*Algorithms need not be software: in the broadest sense, they are encoded procedures for transforming input data into a desired output, based on specified calculations. The procedures name both a problem and the steps by which it should be solved. Instructions for navigation may be considered an algorithm, or the mathematical formulas required to predict the movement of a celestial body across the sky*". Thus, algorithms, like syllogism – the most traditional instrument of judicial reasoning - have a normative function, establishing correlations between a starting set of elements or data, and a precise consequence. Which is the place, then, of algorithms in a judicial proceeding? They not necessarily are incorporated into a software and, moreover, not necessarily are operated automatically: in this sense, it is necessary to move from a conceptual clarification, distinguishing, between different levels of complexity. In fact, in my view, three aspects - validity of the scientific theory; translation of the theory into algorithmic language; fully automated operation of the algorithm – are involved in the application of computational modelling in judicial proceedings, and confusing them may be detrimental for finding effective solutions to the problems tackled here.

From a conceptual point of view, a judicial proceeding and, in particular, a criminal trial, is a process to establish whether and how a fact occurred (actus reus), if such fact has criminal relevance (mens rea), if the defendant perpetrated it and, in such case, provided that the individual is punishable, which is the just penalty to be imposed. This reconstruction follows a flow that is opposed to scientific investigation: while the latter moves form the observation of a set of conditions, trying

[17] Gillespie Tarleton, *The relevance of Algorithms*, in T. Gillespie, P. Boczkowski, K. Foot, *Media Technologies*, MIT Press, Cambridge US, 2014, 167. Such definition has been recently adopted by the study delivered by the Council of Europe on Algorithms and Human Rights: see https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

to explain which are the consequences deriving from them, the judicial decision moves from the consequences (the criminal act) backwards, trying to reconstruct the set of conditions that may have caused the fact. Causality has always been and still remains the core of criminal law, implying the existence of a universal scientific rule or, at least, a validated scientific theory, explaining, beyond any reasonable doubt, the narrative of the criminal fact.

How the recent astonishing achievements in IT and AI impact on such scenario? The answer implies, as said, three steps.

The first layer of complexity encompasses the existence of a universal scientific rule or, at least a validated scientific theory establishing correlations between a set of factors and a precise consequence. Traditionally, it is said that causality should be preferably proved on the basis of a universal rule, establishing that, given A, B will always be the result. However, in light of the achievements of modern science, it is arguable that universal scientific laws do exist at all... In any case, when courts cannot rely on such strong correlation, they must recur to non-universal rules, allowing a certain margin of doubt, at least at the time being. It falls out of the scope to linger over the burgeoning literature focusing on the relationship between science and criminal law: however, although not being the focus of our speculations, this topic is entrenched into the general theme of AI and criminal proceedings, and cannot be overlooked.

It is well-known that, the US Supreme Court delivered a decision in the 90's of the last century that tends to be considered seminal in many jurisdictions, even outside the country, in civil-law legal orders. Daubert v. Merrel Dow Pharmaceuticals[18] established a list of basic standards that the courts, throughout the world, still apply in order to admit evidence based on scientific (or technical)[19] theories. Thus, when reflecting upon the use of computational models in a judicial decision-making process (either at the pre-trial stage, in trial or at sentencing), it must be acknowledged that the first layer of complexity is represented

[18] Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579 (1993).

[19] In fact, Kuhmo Tire extended the Daubert test to technical evidence (Kumho Tire Co. v. Carmichael (97-1709) 526 U.S. 137 (1999)).

by the underpinning scientific theory. A computational model must be rooted into a theory and such theory must meet minimum requirements of validation, according to the peers' community.

The second layer of complexity is consequential, because the results of such scientific theory may be encoded into an algorithm. Acknowledging the definition given above, algorithms design a normative procedure that moves from a set of data towards a desired output, excluding subjective intuitions and arbitrariness from the process. Insofar, it represents a mathematic model,[20] that can be operated by a human being, even in a criminal proceeding, provided that it is based on a sufficiently validated theory and that such theory has been correctly encoded into the algorithm. These two requirements are crucial. In fact, a 'reverse control' on coding is fundamental, because the possibility of reviewing, discussing, challenging the results of an algorithm is a basic condition for a fair decision process and, thus, for a fair criminal proceeding, compliant with fundamental human rights.

The third layer of complexity lays in the fact that the digital turn established two basic and ideal conditions to boost the use of algorithms in every kind of decision-making process. In fact, the stunning amount of data produced (for free) daily by digital devices and the extraordinary and unprecedented computational power now available at a very low cost, represent the ideal context in which algorithms can deliver the most effective results.[21] An algorithm operated by a human being will process a small amount of data, in a relatively long time, delivering few outputs. The same algorithm, operated through a computational model will mine uncountable data in few seconds, delivering an enormous amount of outputs. In this sense, "the use of robots and AI, therefore, is just a special case of the Algorithmic Society. Big Data, too, is just a feature of

---

[20] For an easily-accessible definition of 'models', see O'Neil Cathy, *Weapons of Math Destruction*, Penguin, Allen Lane, London, 2016, § 7.12: to create a model implies making choices about what is important to include into it or not.

[21] See, in general, the remark by Zedner Lucia, *The inescapable insecurity of security technologies?*, in K. Franko Aas, H. Oppen Gundhus, H. Mork Lomel, Technologies of Insecurity. The surveillance of everyday life, Rutledge-Cavendish, Oxon, 2009, p. 257-270 p. 257: "Enormous trust is placed in the capacity of technology to surmount the gravest challenges to our well-being and happiness". "Techno-credulity is widespread".

the Algorithmic Society. Big Data is the fuel that runs the Algorithmic Society... To vary Kant's famous statement, algorithms without data are empty; data without algorithms are blind".[22]

Thus, it is possible to argue that, on the basis of the above-mentioned conditions, algorithms, in their essence of normative, mathematical statements/relations, are gaining momentum over subjectivity at the present day[23]. An algorithmic decision–making process is (or ought to be) opposite an arbitrary one, granting – theoretically - objectivity, accessibility and, ultimately, fairness.[24] However, accessibility implies transparency and transparency is not an innate quality of algorithms. On the contrary, a substantial literature has been focusing on the problem of algorithms' opacity, a condition in which the encoded procedure cannot be validated *ex post*, and thus its results cannot be (even not) explained (and, consequently, not justified).[25]

Having clarified these concepts, it is possible to set a first cornerstone of this study. The need for accessibility is the quintessential aspect in the discourse about the use of algorithm in decision-making processes, both in private and public context. Such accessibility, or transparency, acquires specific implications when it comes to the judicial decision-making process and, in particular, to the criminal trial one. Thus, transparency is the constant issue behind the discourse about the application of algorithms and AI systems to criminal justice. Reflecting on the meaning of such concept, a very crucial distinction has been drawn between explanation and justification.[26] In this sense, much depends, in

---

[22] Balkin Jack M., *The Three Laws of Robotics in the Age of Big Data*, in *SSRN* 2016, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890965

[23] Plesničar Monika M., Sugman Stubbs katja, *Subjectivity, Algorithms and the Courtroom*, in A. Zavrsnik (ed.), *Big Data, Crime and, Social Control*, Rutledge, Abingdon, 2018, (ebook) § 22.37.

[24] The validity of such argument relies on the possibility to really eradicate human biases rather than camouflage them with technology: C. O'Neil, cit., § 7.38.

[25] Geslevich Packin Nizan, Lev-Aretz yafit, *Learning algorithms and discrimination*, in W. Barfield, U. Pagallo, *Research Handbook on the Artificial Intelligence and Law*, Elgar, Cheltenam, 2019, 88 ff.

[26] See recently Hildebrandt Mireille, *Algorithmic Regulation*, cit., 2. (The topic has been deeply debated with regard to the provision of art. 22 GDPR,

the first instance, on the precision of the scientific theory underpinning it and, in the second instance, on the clarity of the language used to translate it into a mathematic formula. To comply with the requirement of explanation, it seems to me that the latter quality is sufficient: a clear mathematic language allows an *ex post* reviewer to understand how the process evolved from the inputs to the outputs. However, to satisfy the need of justification, the underpinning scientific theory must be valid enough to provide a causality relationship between the set of input data and the outputs ('validity' is intended here in the sense provided by the US Supreme Court in the mentioned case of Daubert).

In the light of the previous arguments, it is possible to set also a second cornerstone for this enquiry. Regardless of the different realms of the criminal proceeding in which computational models and AI could be applied, the general impression is that, allowing for the use of the most recent digital achievements in criminal proceedings may deprive courts of their discretion (and the parties of their rights). Delving on this common opinion, two main aspects must be taken into consideration.

First. Irrespectively the correctness of such opinion, what should be ultimately suspected of depriving judges of their power is not 'the machine', rather the algorithm. As said, the normative approach of mathematical modelling is supposed to objectivise a decision process, reducing non-objective criteria or indexes, based on personal culture, biases, shortcuts[27] and contingent conditions. However – second - the algorithmic reasoning is opposed to arbitrariness, not necessarily to discretion. In this sense, the aspiration of introducing algorithms in all sorts of decision-making processes is understandable. In the public sector,

about automated individual decision making, including profile: see Wachter Sandra, Mittlestadt Brent, Floridi Luciano, *Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation*, *International Data Privacy and Law*, 2017, p. 1 -47).

[27] There is extensive literature on heuristics in judicial decision making process. See, in general, the leading text of Kahneman Daniel, Slovic Paul., Tversky Amos (Eds.), *Judgment under uncertainty: Heuristics and biases*, New York 1982, Cambridge University Press.; more recently, Cevolani Gustavo, Crupi Vincenzo, Come ragionano i giudici: razionalità, euristiche e illusioni cognitive, Criminalia 2017, p 181 ff, 182.

such ambition is urged by the need (and the duty, in some jurisdiction)[28] of granting an impartial and fair administration, in any branch of it. In the private sector, excluding arbitrariness in strategic decision, such as hiring one applicant or another, may prove essential in gaining more profit.[29] Nevertheless, two variables must be retained. On the one hand, algorithms can help in achieving such legitimate goals at the conditions mentioned above (first cornerstone): they must underpin a valid theory and be transparent, otherwise they cannot provide impartiality or profit. On the other hand, allowing for the use of algorithms does not imply taking out any discretion from the decision process:[30] there is room for the rulers to regulate the interaction between algorithms and human intuition in a way that does not deprive the process of discretion. This argument is particularly valuable in those contexts in which fundamental rights – such as the one to a fair trial - are in jeopardy and the outcomes of the decision-making process may impact significantly on the individuals' condition (such as the nature and the amount of penalty, depriving them of liberty or even life). Someone may argue that discretion is a risk, rather than a value, when fundamental rights are at stake... Actually, other forms of intelligence, like the artificial one, proved to perform better than the human intuition, in many areas... could this be the case also with judicial decision? Preliminarily, it is worth asking if and how it is possible to scale 'better performances' in judging human criminal behaviour. What would 'better' mean? 'More consistent'? Of course, basic systems of AI can grant high levels of consistency... However, it is questionable if and how far such consistency is a value in criminal proceedings. In fact, as said, courts ruling upon an individual's criminal liability do not perform a scientific or technical process. Judging, in general, and sentencing, in particular, are human tasks not just because they are performed by humans,[31] but because they are intended to be received, understood and accepted by

---

[28] See, e.g. Art. 97 of the Italian Constitution, providing for the duty of impartiality in every branch of the public administration.

[29] With specific regard to law firms, see Katz Daniel M., cit., p. 934.

[30] See Morozov Evgeny, *To Save Everything, Click Here*, Penguins, Allen Lane, London, 2013, § 11.30 (ebook)

[31] See Plesničar Monika M., Sugman Stubbs Katja, *Subjectivity*, cit., § 22.14.

the community:[32] crime is a social construct[33] and the social acceptance of a decision, rather than consistency, is the ultimate task of delivering justice. In this sense, the need for discretion in all the areas of judicial decision (criminal liability, penalty, but also admission and evaluation of evidence) is inherent to the judicial function itself.

For these reasons, the legal discussion must be framed in such terms to detect (and avoid) the conditions in which the use of algorithms can suppress discretion, along with arbitrariness. For example, such situation may happen to occur when algorithms are operated in a totally automated way, without any human intervention. Similar conditions may prove to be detrimental for the fairness of criminal proceedings and, in particular, for the rights of the defence. But this is not a necessary condition. The suppression of the judge's and parties' prerogatives may be a consequence of the characteristics of the algorithm in itself and not of the fact that it is performed by a machine. This distinction is not barely formal. It is part of the necessary premises to address the topic of computational model, AI and criminal law under a legal point of view, because it is inherent to the definition of the risks that need to be considered here.

To summarise, algorithms, incorporated into computational models or not, are pushing on our systems of criminal justice, pledging high rates of efficiency. However, as said, technical and scientific efficiency is a parameter that does not belong to justice. Thus, reliability, accuracy, trustworthiness of such instruments should not be measured only in the terms of computer science:[34] the same concepts have specific meanings in the realm of criminal justice, and they cannot be overlooked. For these reasons, the existing digital methods, having been applied in criminal proceedings - with or without a proper framework

---

[32] See the very famous Introduction of Cardozo Benjamin N., *The nature of the Judicial Process*, Yale University Press, New Haven, 1921, p. 10: "What is that I do when I decide a case? (...) Some principle, however unavowed and inarticulate and subconscious, has regulated the infusion".

[33] See Spector Malcom, Kitsuse John I., *Constructing Social Problems*, 2nd ed., Routlege, London, 2000.

[34] Zavrsnik Aleš, cit.,§ 21.2 warns about the fact that "what counts as 'proper', effective and efficient police work and judicial decision-making has changed"...

of legal regulation - of many jurisdictions, should be reviewed from the legal perspective.[35]

2.2. The protection of fundamental rights

The European countries have strong constitutional traditions. Based on this, the Council of Europe was able to promote the signature and the ratification of the European Convention of Human Rights and the acceptance by the member States of the individual application to the European Court of Human rights. Moreover, the common constitutional traditions are considered a legally binding source of the EU law. Many of those constitutions, along with the ECHR and the Charter of fundamental Rights of the EU, regulate justice, often setting forth specific principles referred to criminal justice. In this sense, the ECHR, the EU law (within the area of the Union competence), and the national constitutions represent a legal filter for any attempt to introduce the use of computational means into criminal proceedings. Nevertheless, the approach to the matter must be neutral: scholars must not move from the prejudice that the use of such means *is* inconstant with fundamental rights... The purpose of a useful study is to assess whether their application may violate some of the principles enshrined in the ECHR. To this aim, it is crucial to establish a shift of perspective: as said, computational models and instruments, software and programs are usually assessed in terms of technical reliability, scaling their performance on the basis of the aspiration to exclude errors or inaccuracy. However, for the reasons summarised above, the endeavour to hybridise (criminal) justice with such means cannot respond to the sole criterion of efficiency. Actually, efficiency, *per se*, is even not expressly mentioned in Art. 6 ECHR. On the contrary, such means should be confronted to the traditional and fundamental principles regulating law enforcement, both in investigation, in trial and in sentencing. The fundamental guarantees set forth by the ECHR, such as the right to private and family life, the presumption of innocence, the equality of arms, must be used as parameters to assess the lawfulness of using automated

[35] Zavrsnik Aleš, cit., § 21.28: These methodologies, are not developed for the study of society, in the manner that statistics in modernity was.

instruments within criminal proceedings or, better, the conditions for a lawful application of it.

Such theoretical approach seems crucial to establish a useful legal discussion in these terms, before rulers fall into the 'digital fascination'. For the reasons that will be sketched out hereinafter, there is a considerable gap between a certain number of common-law countries and Europe, and the latter is still in the phase of 'approaching the topic'. Enumerating the list of digital solutions already adopted in other jurisdictions, acknowledging their existence and, maybe, their performing rates is not enough. It is important to address the problem under the right point of view, that seems to be that of fundamental rights: are such instruments compatible with the presumption of innocence? Are they respectful of the equality of arms? Are all of them compliant with the protection of the right to private and family life within the context of criminal proceedings? An inaccurate analysis of the problem, may lead to endorse computational solutions that, in the long term, may prove even highly inconstant with the essence of fair trial. Allowing such situation would be painful for individuals and, redressing it, extremely challenging for rulers.[36] It is better to adopt a neutral approach and reflect on it before flaws hit the fundamental rights of individuals.

3. Criminal law v. prevention of crime

Based on the previous remarks, it is possible to list some specific topics on which the criminal law scholarship should focus.

Frist and foremost, the union of 'AI' and 'Criminal Law' suggests a dystopic scenario of extremely intrusive means of surveillance, aimed to prevent crime.[37] However, surveillance and prevention fall out of the scope of Criminal Law. The latter regulates the elements of crime

[36] In a general sense, see Morozov Evgeny, cit., § 11.27: "who would be crazy enough to oppose the march of science and suggest that perhaps some of those products need to be modified?

[37] See Franko Aas Katia, Oppen Gundhus Helena, Mork Lomel Heidi, *Introduction*, in K. Franko Aas, H. Oppen Gundhus, H. Mork Lomel, *Technologies of Insecurity. The surveillance of everyday life*, cit., p. 3.

and the consequences of its perpetration. Thus, a criminal proceeding may exist only after a crime has (allegedly) occurred. In this sense, this enquiry is limited to the use of computational models and AI in criminal proceedings and not in policing.

Nevertheless, more and more LEAs are equipped with software predicting where and when crimes are more likely to occur.[38] Recently, the Italian main newspapers reported with great fanfare the introduction of the so called "X Law" software, enabling a more accurate patrolling of the neighbourhoods, on the basis of a set of statistic data. Instruments of 'predictive policing'[39] have been used since a long in many jurisdictions.[40] Setting aside the fascination for it[41] (the Italian journals reported the immediate result of an on-site arrest), such software already demonstrated their limits, 'self-realising' their predictions: in fact, indicating an area as the potential site of crime, will *per se* raise the arrests rates, as more LEA units will be monitoring *that* area. However, the effectiveness of such systems is not an object of this study, because this is not an area of criminal law, and even less of criminal proceedings.

Inherently, the area of prevention of crime and policing – deeply intermingled with intelligence - tends to escape to rigid and precise regulation[42]. Constraining it into strict boundaries would condemn it

---

[38] See. Zavrsnik Aleš, cit.

[39] See extensively, Wilson Dean, *Algorithmic Patrol*, in A. Zavrsnik (ed.), *Big Data, Crime and, Social Control*, cit., § 19.3

[40] See the trial results of Mohler George, Short M.B., Malinowski Sean, Johnson Mark, Tita G.E., Bertozzi Andrea L.,, Brantingham P.J., *Randomised controlled field trials of predictive policing*, in *Journal of the American Statistics Association*, 2015, vol. 510, p. 1399-1411, of an algorithm based on data from American and British jurisdictions about different kind of crimes. In 21 months of testing the algorithm against specialised analysts, the results showed the first being between 1,4 and 2<2 times more accurate than the latter. The group was not totally independent, as two of the members co-founded the company that would commercialise the algorithm, while others served as external counsels for the company.

[41] Zavrsnik Aleš, cit., § 21.13 devotes a paragraph to "crime control and the fascination with numbers".

[42] However, some countries, like Italy, have a long tradition in providing preventive measures, not based on an alleged crime, but actually to avoid the commission of it...

to be less effective... As prevention is a different and autonomous area of criminal justice, the attention here is focused on the specificity of criminal law.

3.1. The specificity of criminal law

Many of the reasons justifying a criminal law approach to the topic have been anticipated in §§ 1 and 2. Because of the values underpinning this area of law, much attention has been paid to it, in the last decades, especially in the second World War aftermath. The idea of recognising the fair trial as a fundamental human right, with some of the most important international bills of rights - such as the International Covenant on Civil and Political Rights and the several regional conventions on human rights – was crucial in strengthening the culture of procedural guarantees, within any branch of the jurisdiction. However, it is with regard to criminal proceeding that the rulers developed the most articulated list of guarantees, establishing the presumption of innocence, but also a very detailed list of minimum standards, deeply influencing the shape of national jurisdictions: from the basic right to access to justice, to the right of having free linguistic assistance, the provisions of the ICCPR and, in particular of the ECHR (thanks to the living-instrument doctrine[43] adopted by the European Court of Human Rights, hereinafter, ECtHR), set forth a relatively strict frame for national legislators. It falls out of the scope of this study to linger over the effective level of harmonisation achieved by the ECHR and by the burgeoning case-law of the Court on criminal fair trail: actually, the real domain of criminal law matters reaches far behind Art. 6, covering, in the broadest sense, also art. 7 (*nulla poena sine lege*), art. 8 (right to private and family life), art. 5 (right to liberty and

[43] Based on a precise reference inserted in the preamble of the Convention - according to which, "the object and the purpose" of the ECHR is not only the maintenance, but also the "further implementation" of human rights and fundamental freedoms, the Court started promoting (since the case of Golder v. UK,21.2.1975) an evolutionary approach, rejecting any originalistic theory in the interpretation of the document. See, Emmerson Ben, Ashworth, Andrew Macdonald Alison, *Human rights and Criminal Justice*, 3rd ed, Sweet and Maxwell, London, 2012. p. 82. 5

security) and arts. 2 and 3, in their procedural aspect (duty to set up an effective investigation on potential violations, respectively, of the right to life and of the prohibition of torture). On the one hand, the wording of the convention regulates, itself, a range of aspects related to the whole criminal proceeding, from the investigations and pre-trial detention, to the execution of penalties, encompassing the principle of legality. And even though the charter does not provide for a precise statute of criminal evidence, Art. 6 (and 8) ECHR establish some crucial benchmarks in the collection and evaluation of it, considered by the ECtHR itself,[44] the realm of national legislators' discretion. On the other hand, as far as the States recognised the right of individuals to apply the Commission - and, eventually, the Court – the Strasbourg case-law started building the wider scheme of a convention-compliant criminal proceeding, that any national ruler must take into account.

The reasons for such comprehensive attention for the criminal jurisdiction are many. In § 1 I highlighted some of the most general features of criminal law, based on which it is possible to argue that criminal law and criminal proceeding can easily be turned into an offensive instrument, punishing and crushing the opponents, the enemies, the weaker, the non-mainstreamers.[45] In fact, basically, criminal law is about the legitimate use of violence by the State.[46] So far, a modern bill of rights cannot overlook the importance of setting strong and precise limitations to the rulers' discretion to regulate criminal affairs, in order to prevent such illiberal outcomes.

Moreover, with the entry into force of the Lisbon Treaty, ten years ago, the European Union experienced both a profound reform of its legal sources and the rationalisation of its competence, acquiring a much detailed and penetrating power in criminal matters, substantive and procedural. Both art. 82 and 83 of the Treaty on the Functioning of the

---

44 See, recently, ECtHR, Svetina v. Slovenia, 22.5.2018.

45 See MacCorkmick Neil, Garland David, *Sovereign States and Vengeful Victims: the Problem of the Right to Punish*, in A. Ashworth, M. Wasik (eds.), *Essays in Honour of Andrew von Hirsch*, Clarendon Press, Oxford, 1998, p. 11-29, p. 28.

46 Duff Antony, Garland David, *Introduction: Thinking about Punishment*, in R.A. Duff, D. Garland (eds.), *A Reader on Punishment*, Oxford University Press, 1994, p. 2 ss.

EU (hereinafter, TFEU) establish that, by means of directives, according with the ordinary legislative procedure, the Union can lay down minimum rules about: (art. 82§2), mutual admissibility of evidence in criminal proceedings; rights of individuals in criminal proceedings; rights of victims of crime; (art. 83), the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension and the approximation of criminal laws and regulations of the Member States if it proves essential to ensure the effective implementation of a Union policy. As a result, in the past decade, a long list of directives was adopted under art. 82§2 to strengthen the procedural rights of the individuals in criminal proceedings. Some of the guarantees already provided by the ECHR have been reiterated in the legal vest of directives - submitted to the interpretation of the CJEU – that the members States have the duty to implement in their jurisdiction, under the consequences provided for in art. 258 and 259 TFEU.

Thus, within the European institutional environment, much attention is paid to the criminal proceedings, as many fundamental rights concentrate in it, the accused person's ones and the victims' ones, at the same time. For this reason, the discourse about the introduction of algorithmic, computational models and AI in the area of criminal proceeding is submitted to the 'filter' of such a rich core of fundamental rights. Behind it, lays the filter of the national regulation, that in some cases is even stricter. In fact, as said, at the national level, the fairness of the proceedings may acquire also another meaning: beyond the interest of the defendant (or the victim), it may be considered an objective guarantee, not only satisfying the defendants' personal interest (actually, they could consider more consistent with their strategy to waive all their rights and accept unfair trial), but also the general interest to the objective fairness in the administration of criminal justice. Despite the opinion and the strategy of the defendant, the system cannot allow unfair criminal proceedings, as this would be inconsistent with its own institutional nature.[47]

Having excluded the area of policing and prevention of crime from the scenario considered here, and highlighted the existence of a

[47] See Ferrua Paolo, *Giustizia del processo, giustizia della decisione*, *Diritto penale e processo*, 2015, 1201 ss.

comprehensive framework of European guarantees surrounding the whole criminal proceeding, it is worth pointing out which aspects of the latter may be more closely affected by the use of computational modelling and AI. Having regard, especially, to the northern American experience - that seems to be the one incorporating most extensively algorithmic and digital solutions in the realm of criminal justice – such tools impact on many phases of the criminal proceeding, from the investigation to the sentencing and the execution of penalties. In the American experience, there seem to be patterns repeating in different stages of the proceeding. In fact, within the considerable span of a proceeding, algorithmic and computational models seem to respond to two main tasks.

First task: a more effective collection of information, to be used either in the investigation and/or as evidence in the trail stage. In this sense, the digital turn offered the LEAs and prosecutors many advantages: an uncountable amount of data to be hacked; much more intrusive hacking systems; a range of information provided by the IoT, 'ready' to be used as evidence in trial. This is the area in which the European criminal justice scenario has been more deeply penetrated by digital solutions. In fact, in many jurisdictions, LEAs simply started using hacking systems to replace traditional interceptions, searches and seizures, almost without a specific regulation. The LIBE Committee (Civil Liberties, Justice and Home affaires) of the European Parliament commissioned a study about Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, delivered in March 2017 by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs. The conclusions of the very comprehensive document focuses the attention on the same crucial aspect highlighted here above. On the one hand, the "discussions that have addressed this topic to some extent have primarily focused on the surveillance activities of the security and intelligence services", and not on the judicial aspect of hacking. Moreover, "these international-level discussions start form the point of view where surveillance activities are necessary and simply require governing laws" [...]: "however, the using of hacking techniques and the implementation of specific legislation at the national level should be subject to EU and international fundamental rights principles. [...] The right for law enforcement agencies to use

hacking techniques should not be assumed but must be deemed necessary within the specific context of a Member State".

Traditionally, this is the area of interaction between criminal proceeding and individual's sphere of private life. In fact, although being extensively protected by one of the most comprehensive regulations in the world (the GDPR), privacy is not an absolute right, even in the European context. When compared with other fundamental interests of the society, such as (in this case) the prosecution of crime, it can be lawfully limited: privacy has its own dimension within criminal proceedings and this is regulated both by the ECHR and the EU law. However, using digitally generated (or hacked) evidence in criminal proceedings may also hinder another fundamental right, to a fair trial: actually, it may violate both the right to a fair trail and the one to private life. In fact, the opacity of the algorithms regulating hacking instruments and other digital devices, generating evidence, may prevent the defence from challenging the accuracy and reliability of it. This can hamper one of the basic aspects of the fair trial, it is to say the equality of arms, that, in its basic meaning implies the right of the parties to challenge the opponent's evidence, not in a theoretical, but in an effective way.[48]

Second task: algorithms and computational models proved useful in several stages of the judicial decision-making process. On the one hand, based on their stunning computational power, such instruments can rapidly mine quintillions of statistic data, helping to establish correlations between the individual's and a social group's behaviour and, apparently, to predict future actions, such as violations of bail conditions or parole or recidivism. On the other hand, thanks to that very same feature, open access digital instruments allow for the complete accessibility of any judicial decision delivered within a jurisdiction and for the searching by key-words (or concepts, with regard to the most recent technical achievements)[49]. Designers of such software claim that the result is

---

[48] Pagallo Ugo, Quattrocolo Serena, *The Impact of AI on Criminal Law and its twofold procedures*, in W. Barfield, U. Pagallo, *Research Handbook on the Artificial Intelligence and Law*, Elgar, Cheltenham, 2019, 400.

[49] Sobowale Julie, *How artificial Intelligence is transforming the Legal profession*, *ABA Journal*, April 2016, referring to NexLP (private company leading the sector) most recent products.

predictability of the decisions, taking into account any individual judge's variables inclinations. In the US, specialised journals often refer to the so called 'science of quantitative legal prediction'. For example, it has been said that trying to predict the Supreme Court decisions seems to be one of the most popular hobbies, at least among politicians and journalists, with very scarce success... But, as the impact of the Court's decisions is crucial for the society as a whole, it seems worth producing accurate models, scoring very high levels of accuracy[50]... Quantitative legal prediction claims to respond with a stunning approximation, to such need.

In this sense, it is possible to argue that the digital turn is promoting predictability as the major feature and aim, at the same time, of criminal justice. On the one hand, predicting defendants' future behaviour; on the other hand, predicting judges' behaviour and decisions. However, the question is whether predictability has an 'autonomous concept'[51] within the realm of criminal law that does not align with the popular meaning of the term.

3.1.1 Moreover, the issue is also related to some of the most crucial and essential aspects of any legal order: the statutory nature of a jurisdiction (impinging on the relationship between judges and the law); the structure of judiciary (regulating the different levels of the jurisdiction and the relationship between lower and superior courts and the role of the latter in assuring the uniformity of the interpretation);

---

[50] See Katz Daniel M., Bommarito Michael J. II, Blackman Josh, *A general Approach for Predicting the Behaviour of the Supreme Court of the United States*, in *SSRN,* 16.1.2017

[51] The term 'autonomous concept' is familiar to the European readers, having been extensively used by both the European Court of Human Rights and the Court of Justice of the European Union. The term indicates that, in the context of these two domains, a notion, applying also in the national jurisdictions, encompasses (also) different aspects and elements. The most known example is the notion of 'criminal charge', having been considered by the court an autonomous concept since the case of Engel and others v. The Nederland, 23.11.1976. For an interesting approach to 'autonomous concepts' see G. Letsas, in European Journal of International Law, 2004, 279-305. As said, also the Court of Luxembourg often applies the interpretative tool of autonomous concepts (sometimes overlapping with those developed by the Court of Human Rights).

the value of the precedent (imposing boundaries on the judges' freedom to divert from it); the concept of 'similarity' between two cases (being the condition to apply *stare decisis*)... The general accessibility to the whole body of decisions in a jurisdiction may seriously impact on two basic characters of the latter. On the one hand, legal systems being not regulated by *stare decisis* – like the majority of the civil-law countries – may witness a shift towards a different pattern, imposing on the courts a duty of specific reasoning in case of over-ruling. The social expectations for full consistency with the 'predicted decision' may urge judges to feel uncomfortable in departing form it, seriously impinging on the independence of judiciary.[52] Moreover, mining a mass of data, predictive models may not distinguish between lower courts and superior courts' decisions, hampering the institutional structure of justice itself... These are all crucial aspects in determining the concept and the value of predictability, being deeply rooted in the most inherent aspects of the common-law and civil-law traditions. As such, they affect all branches of a legal system, and not only criminal justice. However, the concept of predictability has a specific meaning within the modern conception of the principle of legality. The theory of predictability of criminal commands and penalties moves from the liberal theory of criminal law and finds a beacon in the famous Bentham's critique of the British judges.[53] Men can understand the consequences of their behaviour and are able to self-determine: for these reasons, the rulers must put them in the condition to foresee, clearly and surely, the penal consequences of a behaviour before putting it into action.[54] It is worth asking whether this is the very same aim and function promised by computational models mining and analysing all the decisions in a jurisdiction, searching for patterns of correspondence between decisions and judges' behaviour.

These arguments confirm the specificity of the realm of criminal justice within the general context of 'legal AI'. Criminal law and criminal

---

[52] See the European Ethical Charter for the Use of AI in the systems of justice. Annex II, delivered in December 2018 by the CEPEJ (Council of Europe).

[53] Bentham Jeremy, *Works,* V, edited by J. Bowring, Edinburgh 1843.

[54] Cadoppi Alberto, *Il valore del precedente*, cit., p. 65 s.

proceeding are a branch of regulation in which the issue of the use of computational modelling and AI need to be addressed specifically.

3.2 The specificity of Europe

A second aspect of specificity is geographical. There exist a lag between the US (and some others common-law jurisdictions, such as some Australian ones)[55] and Europe, under the view-point of massive reliance on digital solutions in justice systems.[56] Over two decades,[57] new branches of research and scholarship developed in the US, often bringing computer scientists and, in particular, modelling developers, to see a potentially rich new market for their software in the realm of justice...[58] and Europe seems to be a virgin soil.[59] In fact, at the time being, "the use of predictive tools in criminal trials is very rare in Europe"[60] as many other algorithmic instruments are,[61] and there is room to set up a legal discussion, before the market rules overarch any effective possibility for it.

---

[55] See the Australian Report in the study, A framework for hacking by law enforcement, cit., p. 111.

[56] For a complete overview of American leading law-firms having turned to technological resources for the accomplishment of traditional tasks, Li Victor, *Techtrekkers*, *ABA Journal*, April 2016, p. 37-43.

[57] See Sobowale Julie, *Beyond Imagination*, *ABA Journal,* April 2016, p. 47-53, p. 47: "the future of legal professions started twenty years ago", referring to Discovery Cracker, the first software for legal researches.

[58] The initiative of pinpointing instances of AI in judicial systems almost came from the private sector: see, European Ethical Charter for the use of AI in judicial systems and their environment. Appendix I, p. 14.

[59] See Sobowale Julie, *How artificial intelligence*, cit., reporting Adam Nguyen, EBrevia's co-founder (supplying legal software based on machine learning), interest in covering the European market.

[60] See, European Ethical Charter, cit., p. 37: with the exception of HART (Harm Assessment Risk Tool), being under experimentation at the moment in some UK jurisdiction, there is no knowledge of other similar instruments.

[61] See, e.g. S.F. Ward, Doing It with Data, in ABA Journal, September 2018, p. 38, about the so-called Priori system, a platform that pairs attorneys with clients based on detailed experience information. The service is free for the attorneys who agree to discount 25% hourly rates, while clients pay 10% of the reduction to Priori.

As to the reasons for such a lag, they seem to be multi-fold. The main element is that, the US represent, in the Western world, the country that most extensively invested in computational sciences, leading the digital revolution. Social and cultural issues are at the basis of such trend and they have been studied in several branches of scholarship. Under the economic point of view, a predominance of the private sector over the public one seems to having been the most relevant input. Similarly, the US scenario seems to be positively affected by the coexistence of strong private and public research sectors. This condition enhanced the development of a competitive environment, promoting a faster and wider application of computational modelling also in social sciences.[62]

A second element is but legal, and it is twofold. First. The areas of private and criminal justice are inherently distinct in any jurisdiction, as the latter is mostly based on oral hearings. This is true also in the US.[63] However, the massive number of guilty pleas reduces remarkably the room for oral trials in front of the courts, reducing the oral activity at the disposition hearing, in which the judge delivers a decision on sentencing. This trend caused a 'bureaucratic effect', transforming the oral hearing – being traditionally the stage for intense, human performances, into a more bureaucratical proceeding, concentrating the judicial discretion in the sole moment of sentencing. In such a context, the need for a more efficient management of data became relevant, inducing an enlargement of the recurs to risk assessment methods.

Second. The turn of the American penal doctrine from a rehabilitative paradigm to the idea of 'just desert',[64] deeply influenced the discourse

---

[62] See the comprehensive analysis of Susskind Richard, *The End of Lawyers?*, OUP, Oxford 2008; see also Katz Daniel M., *Quantitative Legal Prediction*, cit., pp. 909 ff.

[63] See Christin Angèle, *Algorithms in practice*, cit., p. 8 reporting an interview with a clerk in an American local court: "here at the criminal side it's messy... It's not like on the civil side. Lawyers, Das, they negotiate, they decide on the plea... They do not kwon what's going to happen. They scribble down notes on paper sheets, they couldn't switch to paperless!".

[64] See Dubber Markus, Hörnle Tatyaina, *Criminal Law. A Comparative Approach*, OUP, Oxford, 2016, 4. The same trend, however, affected also the English system: see Padfiled Nicola, Morgan Rod, Maguire Mike, *Out of Court, out of sight? Criminal sanctions and non-judicial decision-making*, in M. Maguire, R.

about incarceration and inhabilitation, determining increasing rates of incarcerations.[65] This implied, on the correctional point of view, more room for the development of computational models meant to grant a more objective and effective management of the stage of the execution of penalties.

In Europe, the use of negotiated justice is not predominant. Although the majority of the European jurisdictions provide for some kind of negotiation between the prosecution and the defence,[66] almost based on a reduction of the sanction against a very early definition of the proceeding, the trial still represents the most common development in criminal cases, leaving room for oral hearings, with oral discussion and oral presentation of evidence... More unpredictable variables distinguish the typical European criminal court context from the American one. At the same time, European jurisdictions are strongly rooted into the rehabilitation doctrine: the blueprint of correctional policies is theoretically based on individualised approach, against the efficiency model promoted in the US.

In conclusion, I suggest that, for the reasons presented above, the European context must be considered an autonomous area of investigation within the discourse about computational models, AI and systems of criminal justice, especially because of the remarkable framework for the protection of fundamental rights, established in Europe in the second WW aftermath.

3.3 Specific implications of stare decisis

However, within the European scenario itself, there are other specificities that may impinge on the reflection about if and how

---

Morgan, R. Reiner (eds.), T*he Oxford Handbook of Criminology*, 5th ed., OUP, 2012, (955-985) p. 974.

65 Wacquant Loic, *The great penal leap backward: Incarceration in America from Nixon to Clinton*, in J. Pratt, D. Brown, M. Brown, S. Hallsworth, W. Morrison (eds.), T*he New Punitiveness. Trends, theories, perspectives*, Willan Publishing, Cullompton, 2005, p. 5 (3-26), reporting the US incarceration rate being, since the early 70s of the last Century, two or three times that of the major European countries.

66 Quattrocolo Serena, Ruggeri Stefano (eds.), Personal participation in criminal proceedings, Springer 2019, p. 467.

computational models and AI should be used in criminal proceedings. An important distinction exists between common-law and civil-law jurisdictions, having important repercussion on the topic at stake.

As said, one of the most remarkable effects of the use of computational model in justice systems is the impact of predictability – praised by the many advocates of open data instruments, but also deeply coveted by lawyers – on the value of the precedent. Under this point of view, the English system traditionally relies on the principle of *stare decisis* which is mostly unfamiliar to the civil law tradition. Goodhart considered it "the distinctive feature of the common law system", and, thus, the "fundamental distinction between the English and the Continental legal method".[67] Despite the progressive realignment between the two legal families, over the years, having been theorised by the some of the most prominent comparativists,[68] this aspect still plays a remarkable distinction between the English jurisdictions and the continental ones.[69] Although there is no room for a more accurate reconstruction here, it is worth highlighting that the absence of *stare decisis* reflects a different structure of the higher Courts on the continent, which is inherent to the analysis that will follow. The number, the inner divisions, the functions of continental higher court is unavoidably intermingled with the value and the role of the precedent: the civil law 'model' implies a more diffuse authority of those organs and their decisions.[70] Moreover, the continental courts cannot rely on the writ of certiorari and have to hear – in a general sense - all the cases brought before them... and huge numbers mean less accessibility![71] The relevance of such remark is patent. Delving on the

---

[67] Goodhart Arthur L., *Precedent in English and Continental Law*, in *Law Quarterly Review*, 1934, 40-65, p. 42.

[68] Zweigert Konrad, Kötz Hein, *Einfürung in die Rechtsvergleichung, auf dem Gebiete des Privatsrechts*, I, JCB Mohr Verlag, Tübingen, 1971, p. 314 ff.

[69] See Cappelletti Mauro, *The Doctrine of Stare Decisis and the Civil Law: A Fundamental Difference – or no Difference at All?*, in H. Bernstein, U. Drobnig, H. Kötz, *Festschrift für Konrad Zweigert zum 70. Geburstag*, JCB Mohr Verlag, Tübingen, 1981, p. 383.

[70] Cappelletti Mauro, The Doctrine, cit., 383.

[71] Although not recent, an enlightening work is that collected in a special number of the Revue international de droit comparé, by Bellet Pierre, Tunc André, Touffait Adplphe, *La cour judiciaire suprème*, Economica, Paris, 1978.

value of predictability implies distinguishing between the common law system courts and the civil law ones. Also recruitment and conditions of independence of judiciary are crucial for this topic.[72] The continental tradition of the bureaucratic state deeply influenced the structure of judiciary in the main European countries allowing for the Montesquieu's classical theory to flourish: judiciary still is, in many of those countries, an independent body of civil servants, recruited by public selection, who will progress in their career based on seniority, a feature that still marks a deep difference with the Anglo-American system, especially with regard to the highest courts.[73] The sketched background justifies the fact that the continental judge "develops skills in technical rather than in policy-oriented decision-making.[74] In such context, the civil law supreme court judges tend towards anonymity and their names do not emerge in bold relief.

However, it is worth highlighting that, comparing the European scenario with the US one, from the angle of the use of AI in criminal law, some further distinctions are due within the European area it-self. Some European jurisdiction provide for a jury trial, at least in some most serious cases, based on the traditional bifurcation between adjudication (fact finding) and ruling matters of law.[75] One of the latter is sentencing,

---

See, in particular, on this point, Tunc André, Conclusion: la cour supreme idéale, p. 441 ff.

[72] See Zweigert Konrad, Kötz Hein, *Einfürung in die Rechtsvergleichung*, cit., p. 139 (this part of the book is reproduced and translated into the English edition, by T. Weir, *An Introduction to Comparative Law*, OUP, 1998, p. 124 ff.); For a more recent overview on some of the most influential European jurisdictions, see, Delmas-Marty Mireille, Spencer John (eds.), *European Criminal Procedures*, Cambridge University Press, Cambridge 2002, 81 ff.

[73] Cappelletti Mauro, *The Doctrine*, cit., p. 387 and 393, where he affirms that the topic of confronting the two traditions needs to be approached under multi-fold aspects: "institutions and their organisations, bias and traditions, sociological backgrounds and attitudes of those who run the 'machinery'".

[74] See Cappelletti Mauro, cit., p. 387.

[75] See Langbein John H., *Bifurcation and the bench*, in P. Brand, J. Getzler, *Judges and Judging in the History of the Common Law and Civil Law*, Cambridge University Press, Cambridge, 2012. p. 67 ff. (See the interesting critical remark: "A judge who is kept away from fact-finding is so remote from the core function of adjudication that he is only peripherally responsible for the court's decision."

applying the just penalty to convicted. At the present time, the distinction between verdict and sentence is very clear in the Anglo-American criminal jurisdictions (see England for the most serious cases, before the Crown Court),[76] where the judge determines the sanction after the fact finding has been dealt with. However, this cannot be considered a distinguishing feature of the common-law, as some European continental countries, like France, provide for jury verdict, for serious cases, followed by judicial sentencing.

For the purposes of this study, the topic has a specific relevance. In fact, courts in sentencing, may rely on a different set of information, from the one used for fact-finding.[77] On the one hand, there may be insufficient factual evidence, if the trial concentrated on legal issues. On the other hand, there may be no trial and no formal evidence at all, as a consequence of a guilty plea. Determining the basis for sentencing is crucial and in some jurisdictions there may be exclusions, from the file, of information and materials that could be relevant in sentencing, but cannot be considered for the fact-finding decision-making process. This is the case of psychological assessment, that, in some jurisdictions, like Italy, for instance, is prohibited in fact-finding and allowed only at the correctional stage.[78]

This could be an example of limitation in using tools predicting violent behaviour and recidivism. As said above, such software are rooted into a psycho-criminological theory, whose scientific reliability must be assessed in court. Nevertheless, no evaluation based on

---

[76] A full reconstruction of the English sentencing powers falls out of the scope here. Two aspects are worth highlighting, in these general remarks: on the one hand, the huge range of cases in which criminal sanctions are not applied by courts, rather by other public "agents who also have the role of keeping order, investigation, or preparing cases for prosecution". On the other hand, having regard to formal sentencing, the "relentless frequency" of the sentence legislation over the recent years, beside the growth of guidelines, delivered today by the Sentencing Council, established by the Coroner and Justice Act 2009 (Ashworth Andrew, *Sentencing and Criminal Justice*, 6th ed., Cambridge University Press, Cambridge, 2015, p. 12 and 21).

[77] See Ashworth Andrew, *Sentencing*, cit., p. 424.

[78] Art. 220.2 of the Code of criminal procedure prevents expert witness on character (allowing it for psychiatrics) during the trial stage. It is allowed at the correctional stage.

psycho-criminological assessment would be admitted, e.g., in Italy, for fact finding and sentencing.

4. Conclusions

This general overview was aimed to focus the attention on the most relevant risks hidden in the 'uncontrolled' action of computational modelling and AI interaction on the criminal law realm, with regard to the civil law jurisdictions and, in particular, to Europe. As said, at the time being, the rush is not in giving answers but in starting posing the right questions. Why do we need computational modelling and AI in our court rooms? Can they improve the quality of criminal justice? Is this compliant with fundamental rights?

Answering these questions means urging criminal lawyers to focus their attention on an unknown realm, making an effort to understand risks and potentialities of the application of AI to criminal justice. It is undisputed that criminal law will not be excepted by the effects of the more sophisticated developments of the digital turn: like any other area of law, also criminal law must deal with it. The rights approach seems to me not that of rejecting it, but to understanding advantages, limits and risks of it. The European jurisdictions can rely on a strong net of fundamental rights and procedural guarantees, deriving from the ECHR, the EU law and the national constitutions. Based on this, European criminal lawyers can face the new challenges of the so-called fourth revolution with the hope of preventing the risk of serious violations of fundamental rights, such as the presumption of innocence, the fair trial, the right to private life and, maybe, of exploiting the benefits that the AI may bring to our backlogged justice systems.

Bibliography

ASHWORTH, Andrew. Sentencing and Criminal Justice, 6th ed., Cambridge University Press, 2015.

BALKIN JACK, M. The Three Laws of Robotics in the Age of Big Data, in SSRN 2016, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890965

BELLET PIERRE, TUNC, André, TOUFFAIT, Adolphe. La cour judiciaire supreme, Economica, Paris, 1978

BENTHAM JEREMY, Works, V, edited by J. Bowring, Edinburgh 1843.

BLACK, Julia. Critical Reflections on Regulation, in Australian journal of legal Philosophy 2002, vol. 27, 1-36

BOISTER, Nicholas. An introduction to Transnational Criminal Law, 2nd ed., OUP 2018

CADOPPI, Alberto. Il valore del precedente nel diritto penale. 2nd ed., Giappichelli, Torino, 2014

CAPPELLETTI, Mauro. The Doctrine of Stare Decisis and the Civil Law: A Fundamental Difference – or no Difference at All, in H. Bernstein, U. Drobnig, H. Kötz, Festschrift für Konrad Zweigert zum 70. Geburstag, JCB Mohr Verlag, Tübingen, 1981.

CARDOZO, Benjamin. The nature of the Judicial Process, Yale University Press, New Haven, 1921

CEVOLANI, Gustavo; CRUPI, Vincenzo. Come ragionano i giudici: razionalità, euristiche e illusioni cognitive, Criminalia 2017, p 1-29.

CHRISTIN, Angèle. Algorithms in practice: Comparing web-journalism and criminal justice, in Big Data and Society, 2017 (July-December), p. 1-14.

DELMAS-MARTY, Mireille; SPENCER, John (eds.). *European Criminal Procedures*, Cambridge University Press, Cambridge 2002.

DUBBER, Markus; HÖRNLE, Tatiana. Criminal Law. A Comparative Approach, OUP, Oxford, 2016

DUFF, Antony; GARLAND, David. Introduction: Thinking about Punishment, in R.A. Duff, D. Garland (eds.), A Reader on Punishment, Oxford University Press, 1994, p. 2-50.

EMMERSON, Ben; ASHWORTH, Andrew; MACDONALD, Alison. Human rights and Criminal Justice, 3rd ed, Sweet and Maxwell, London, 2012.

FERRUA, Paolo. Giustizia del processo, giustizia della decisione, Dir. pen. proc. 2015, p. 1201-1209.

FLORIDI, Luciano. The Fourth Revolution, OUP, Oxfrod 2017

FRANKO, Aas Katja; OPPEN, Gundhus Helene; MORK, Lomel Heidi. Introduction, in K. Franko Aas, H. Oppen Gundhus, H. Mork Lomel, Technologies of Insecurity. The surveillance of everyday life, Rutledge-Cavendish, Oxon, 2009, p. 257-270

GARAPON, Antoine. LASSÈGUE, Jean. Justice digitale, PUF, Paris, 2018

GESLEVICH, Packin Nizan; LEV-ARETZ, Yafit. Learning algorithms and discrimination, in W. Barfield, U. Pagallo, Research Handbook on the Artificial Intelligence and Law, Elgar, Cheltenam, 2019, p. 88-113

GILLESPIE, Tarleton. *The relevance of Algorithms*, in T. Gillespie, P. Boczkowski, K. Foot, *Media Technologies*, MIT Press, Cambridge US, 2014

GOODHART, Arthur L. Precedent in English and Continental Law, in Law quarterly Review 1934, p. 40-65.

HILDEBRANDT, Mireille. Algorithmic Regulation and the Rule of Law, Phil. Trans. R. Soc. 2018, p. 1-8.

KANEMAN, Daniel; SLOVIC, Paul. Tversky Amos(Eds.) (1982). Judgment under uncertainty: Heuristics and biases. New York: Cambridge University Press.

KATZ, Daniel M.; BOMMARITO, Michael J. II; BLACKMAN, Josh. A general Approach for Predicting the Behaviour of the Supreme Court of the United States, in SSSRN, 16.1.2017

KATZ, Daniel M.; Quantitative Legal Prediction, Or- How I Learned to Stop Worrying and Start Preparing for the Data-Driven Future of the Legal Services Industry, in Emory L.J. 2013, p. 909-966

KURZWEIL, Ray. The Singularity is Near, Viking, New York, 2005

LANGBEIN, John H. Bifurcation and the bench, in P. Brand, J. Getzler, Judges and Judging in the History of the Common Law and Civil Law, Cambridge University Press, 2012. p. 67-82

LETSAS, George. The Truth I Autonomous Concepts, in European Journal of International Law, 2004, p. 279-305

LI VICTOR, Techtrekkers. in ABA Journal, April 2016, p. 37-43.

MACCORKMICK, Neil; GARLAND, David. Sovereign States and Vengeful Victims: the Problem of the Right to Punish, in A. Ashworth, M. Wasik (eds.), Essays in Honour of Andrew von Hirsch, Clarendon Press, Oxford, 1998, p. 11-29.

MOHLER, Geroge O.; M.B. Short; MALINOWSKI, Sean; JOHNSON, Mark; G.E.Tita; BERTOZZI, Andrea L.; BRANTINGHAM, Jeffry P. Randomised controlled field trials of predictive policing, in Journal of the American Statistics Association, 2015, vol. 510, p. 1399-1411

MOROZOV, Evgeny. To Save Everything, Click Here, Penguins, Allen Lane, London, 2013, § 11.30 (ebook)

NEGROPONTE, Nicholas. Being Digital, Hodder&Stoughton, London 1995

NIEVA, Fenoll Jordi. Inteligencia artificial y proceso judicial, Marcial Pons, Madrid, 2018.

O'NEIL, Cathy. Weapons of Math Destruction, Penguin, Allen Lane, London, 2016

PADFILED, Nicola; MORGAN, Rod; MAGUIRE, Mike. Out of Court, out of sight? Criminal sanctions and non-judicial decision-making, in M. Maguire, R. Morgan, R. Reiner (eds.), The Oxford Handbook of Criminology, 5th ed., OUP, 2012, p. 955-985

PAGALLO, Ugo; QUATTROCOLO, Serena. The Impact of AI on Criminal Law and its twofold procedures, in W. Barfield, U. Pagallo, Research Handbook on the Law of Artificial Intelligence 2018, Edgar Elgar, p. 385-409.

PLESNIČAR, Monica M.; SUGMAN, Stubbs Katja. Subjectivity, Algorithms and the Courtroom, in A. Zavrsnik (ed.), Big Data, Crime and, Social Control, Rutledge, Abingdon, 2018, (ebook) § 22.37.

QUATTROCOLO, Serena; RUGGERI, Stefano (eds.). Personal participation in criminal proceedings, Springer 2019.

RISSLAND, Edwina L.; ASHLEY, Kevin D.; LOUI, R.P. AI and Law: A fruitful synergy, in Artificial Intelligence 2003, Special Issue, 2.

SIEBER, Ulrich. Computerkriminalitaet und Strafrecht, Carl Haymanns Verlag, Koeln, 1977

SIEBER, Ulrich. Mastering Complexity in the Global Cyberspace: the Harmonisation of Computer-Related Criminal Law, in M. Delmas Marty, M. Pieth, U. Sieber (eds), Les Chemins de l'harmonisation pénale, 2008, p. 127-140.

SOBOWALE, Julie. Beyond Imagination, in ABA Journal, April 2016, p. 47-53

SOBOWALE, Julie. How artificial Intelligence is transforming the Legal profession, ABA Journal, April 2016

SOLUM, Lawrence. Legal Personhood for artificial intelligences, in North Carolina Law Review, 1992, p. 1231-1288

SPECTOR, Malcom; KITSUSE, John I. Constructing Social Problems, 2nd ed., Routlege, London, 2000.

SUSSKIND, Richartd. The End of Lawyers?, OUP, Oxford 2008

WACHTER, Sandra; MITTLESTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation, International Data Privacy and Law 2017, p. 1 -47

WACQUANT, Loic. The great penal leap backward: Incarceration in America from Nixon to Clinton, in J. Pratt, D. Brown, M. Brown, S. Hallsworth, W. Morrison (eds.), The New Punitiveness. Trends, theories, perspectives, Willan Publishing, Cullompton, 2005, p. 3-26.

WARD, Stephanie Francis. Doing It with Data, in ABA Journal, September 2018, p. 38

WILSON, Dean. Algorithmic Patrol, in A. Zavrsnik (ed.), Big Data, Crime and, Social Control, Rutledge, Abingdon, 2018, (ebook).

ZAVRSNIK, Aleš (ed.). Rutledge, Abingdon, 2018, (ebook)

ZEDNER, Lucia. The inescapable insecurity of security technologies?, in K. Franko Aas, H. Oppen Gundhus, H. Mork Lomel, Technologies of Insecurity. The surveillance of everyday life, Rutledge-Cavendish, Oxon, 2009, p. 257-270

ZWEIGERT, Konrad; KÖTZ, Hein. Einfürung in die Rechtsvergleichung, auf dem Gebiete des Privatsrechts, I, JCB Mohr Verlag, Tübingen, 1971.

Informações adicionais e declarações dos autores
(integridade científica)

Declaração de conflito de interesses (conflict of interest declaration): a autora confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores.

Declaração de ineditismo e originalidade (declaration of originality): a autora assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 02/09/2019
- Controle preliminar e verificação de plagio: 05/09/2019
- Avaliação 1: 27/9/2019
- Avaliação 2: 29/9/2019
- Decisão editorial preliminar: 29/9/2019
- Retorno rodada de correções: 05/10/2019
- Decisão editorial final: 08/10/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editoras-associadas: 2 (CC e BC)
- Revisores: 2

COMO CITAR ESTE ARTIGO:

QUATTROCOLO, Serena. An introduction to ai and criminal justice in Europe. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1519-1554, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.290

A Inteligência Artificial e a disputa por diferentes caminhos em sua utilização preditiva no processo penal

The Artificial Intelligence and the dispute for different ways in its predictive use in the criminal process

Rodrigo Régnier Chemim Guimarães[1]

Universidade Positivo - Curitiba/Paraná

rrchemim@hotmail.com

http://lattes.cnpq.br/3509382891487960

http://orcid.org/0000-0001-7378-4553

Resumo: O artigo explora a disputa entre dois modelos globais em torno da aceitação da inteligência artificial para pesquisas preditivas de decisões de juízes e tribunais, com especial enfoque no âmbito do processo penal. Enquanto nos Estados Unidos a pesquisa é livre e vem se desenvolvendo, na França houve criminalização do comportamento de quem se utilizar de decisões judiciais para tanto. Considerando a delicada cooperação entre peritos em processo penal e engenheiros do conhecimento na construção dos algoritmos que irão ensinar a máquina nas pesquisas preditivas, qual dos dois caminhos seria o adequado? A disparidade de premissas interpretativas no processo penal coloca em risco possíveis construções silogísticas que possam partir de entimemas? O uso de inteligência artificial na análise preditiva de decisões processuais penais viola ou assegura garantias constitucionais? Levando em conta essas questões, o artigo pretende avaliar se o modelo liberal norte-americano seria a melhor opção, sem olvidar de alguns alertas já identificados pela Comissão Europeia para a eficácia da Justiça, em sua recente "Carta Ética Europeia de Utilização da Inteligência Artificial nos Sistemas Judiciários e seu Entorno", notadamente quanto aos riscos

[1] Doutor em Direito de Estado pela UFPR. Professor Titular de Direito Processual Penal na graduação e no Mestrado Profissional em Direito na Universidade Positivo, em Curitiba, Paraná. Procurador de Justiça no Ministério Público do Estado do Paraná.

de prevalências de preconceitos que possam estruturar equivocadamente as pesquisas preditivas e seus resultados.

Palavras-Chave: inteligência artificial; predição; silogismos; processo penal.

Abstract: *The article explores the dispute between two global models about the acceptance of artificial intelligence to carry out predictive research around judges and courts, with special focus on criminal procedures. While in the United States research is free and has been developing, in France there has been recent criminalization of the behavior of those who use judicial decisions to do so. Given the delicate cooperation that must exist between experts in criminal procedure and knowledge engineers in the selection and construction of the algorithms that will teach the machine for the preparation of the predictive research, which one would be appropriate? The disparity of interpretative premises in the criminal process put in risk some possible syllogistic constructions that may arise from entimemas? Does the use of artificial intelligence in predictive analysis of criminal procedural decisions violate or ensure constitutional guarantees? Taking these issues into account, the article aims to evaluate whether the US liberal model would be the best option, without forgetting some alerts already identified by the European Comission for the effectiveness of Justice in its recent "European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and its Environment", notably regarding the risks of prevalence of prejudices that may misrepresent predictive research and its results.*

Keywords: *Artificial Intelligence; prediction; syllogisms; criminal proceedings.*

Introdução

Ainda que as experiências pioneiras e posteriores a Alan Turing no uso da inteligência artificial datem já de mais de meio século, foi apenas quando de sua conjugação com a facilitação do acesso à rede mundial de computadores, nos últimos vinte anos, que ela ganhou impulso decisivo a ponto de vir se inserindo paulatinamente no cotidiano das pessoas. Seu emprego hoje facilita a pesquisa sobre qualquer assunto, cataloga preferências, organiza perfis de consumo, seleciona propagandas, difunde ideias, formata e pasteuriza opiniões, promove censuras, direciona debates e até mesmo realiza ações concretas no mundo físico, a exemplo de acender e apagar a luz, ligar e desligar um aparelho, pesquisar uma música, o clima ou qualquer outro assunto. O avanço é de tal ordem que uso da inteligência artificial permite estabelecer um diálogo programado entre a máquina e o ser humano, como se dá com a assistente virtual Alexa, da empresa Amazon e suas correlatas. A sociedade já não parece mais ser capaz de se desenvolver sem o emprego da inteligência artificial. É uma tecnologia que veio para ficar e se expandir em modo que há poucos anos somente era imaginado em livros ou filmes de ficção científica.

Compreender como tudo isso impacta no direito processual penal e como será possível usufruir da inteligência artificial na melhoria do desempenho processual é inevitável e urgente. Já se sabe que são inúmeras as possibilidades de uso da inteligência artificial no processo penal, desde o consolidado auxílio em pesquisa jurisprudencial, passando pela produção e valoração probatórias, elaboração de petições e juízos de admissibilidade de recursos extraordinários[2]. Uma delas em particular vem gerando não apenas controvérsia, mas até mesmo providência legislativa: trata-se da função preditiva que o uso da inteligência artificial pode promover em torno das decisões judiciais no âmbito processual.

São dois os caminhos que parecem se estruturar até aqui. De um lado, levando em conta a necessidade de preservação da intimidade dos julgadores e as críticas do filósofo francês Eric Sadin no sentido de que o uso irrefletido da inteligência artificial pode conduzir à "emergência

[2] Sobre cada um destes aspectos vide NIEVA FENOLL, Jordi. *Inteligencia artificial y proceso judicial*. Madrid: Marcial Pons, 2018, *passim*.

de um novo regime de verdade"[3], computam-se os riscos que uma pesquisa preditiva possa gerar caso não se leve em conta que as máquinas são alimentadas por seres humanos e, nessa medida, os resultados das pesquisas podem advir de preconceitos. De outro, a necessidade de ampliar quadros de compreensão de como operam os processos decisórios das Cortes de Justiça, reforçando a ideia de publicidade das decisões e respectivo "accountability", incorpora-se à abordagem defendida pelos matemáticos Cristian Calude e Giuseppe Longo ao ponderarem o quanto os algoritmos podem auxiliar na promoção de uma melhor prestação jurisdicional[4]. Mais alinhados a essa segunda corrente, os norte-americanos, por exemplo, vêm utilizando a inteligência artificial como ferramenta para predizer processos decisórios já há algum tempo, fazendo-o com certa dificuldade, porém, com relativo sucesso, sem que isso tenha gerado a necessidade de regulamentação legal. Em sentido oposto, os franceses recentemente editaram uma lei tipificando como crime quem resolver coletar dados para esse tipo de análise.

Os radicalismos em geral costumam ser equivocados e não é raro que para suprir esse olhar dicotômico acabe surgindo um meio-termo que equilibre aspectos positivos e negativos de ambos os extremos. Esse, inclusive, parece ser o caminho que vem sendo proposto pela Comissão Europeia para a Eficácia de Justiça – CEPEJ. A questão é saber se é possível identificar um percurso ideal a ser trilhado, pois, não obstante a tecnologia ainda não tenha desenvolvido toda sua potencialidade, vem sendo concretamente empregada em diversos países. Entre estas duas posições vigentes, então, qual será o melhor caminho a se seguir? O uso de inteligência artificial na análise preditiva de decisões processuais penais viola ou assegura garantias constitucionais? Entre a privacidade do julgador e o risco de produção de novos "discursos de verdade", de um lado, e a publicidade processual somada à prestação de contas jurisdicional com melhorias para a segurança jurídica, de outro, o que deve prevalecer? Qual o risco de se ter uma construção dos algoritmos a partir de um entimema,

---

[3] SADIN, Eric. *Intelligence Artificielle ou l'enjeu du siècle (L')*: Anatomie d'un antihumanisme radical. Paris: L'Echappée, 2018, p. 81.

[4] CALUDE, Cristian; LONGO, Giuseppe. The Deluge of Spurious Correlations in Big Data. In: *Foundations of Science*. Vol. 22, Issue 3, DOI 10.1007/s10699-016-9489-4, 2017, pp. 595-612, p. 611.

ainda mais quando não ficarem preestabelecidas, de forma clara, qual das diferentes correntes dogmáticas do processo penal foi adotada?

Para nortear a discussão em torno dessas questões se vai à fonte criadora da tecnologia, incursionando no modo como ela se estrutura e se organiza. Parte-se, então, da visão de Alan Turing, considerado o pioneiro na criação da inteligência artificial nos anos 1950, na compreensão e na utilização dos algoritmos no ensinamento das máquinas. Leva-se em conta também a divisão consagrada pelo filósofo John Searle entre inteligência forte e fraca, para limitar o campo de utilização da nova tecnologia. Segue-se ampliando o olhar para os fundamentos filosóficos aristotélicos em torno do método silogístico que embasa o ensinamento da máquina para alcançar o conhecimento, procurando estabelecer os limites e perigos que se tem pela frente.

Por fim, se ingressa na discussão entre os dois modelos de utilização da inteligência artificial preditiva das decisões dos magistrados no âmbito processual penal, analisando, igualmente, o percurso que vem sendo empregado pela Comissão Europeia para a Eficácia de Justiça – CEPEJ para estabelecer os melhores fundamentos que possam auxiliar uma eventual tomada de posição a esse respeito no Brasil.

1. O "jogo da imitação" e a divisão da inteligência artificial em "fraca" e "forte".

Ainda que o espaço e o escopo, aqui, não permitam aprofundar teorias computacionais, para estabelecer as possibilidades de uso democrático da inteligência artificial na predição de decisões no processo penal é preciso ter presente como ela opera.

Ao formular sua ideia original em torno do que depois se denominou de "inteligência artificial"[5], Alan Turing propôs ilustrá-la através

[5] A expressão "inteligência artificial" é atribuída a John McCarthy que, em 1955, a definiu como a ciência de "fazer com que uma máquina tenha um comportamento tal que ele seria chamado de inteligente caso fosse realizado por um ser humano". Conforme MCCARTHY, John; MINSKY, Marvin L.; ROCHESTER, Nathaniel; SHANNON, Claude. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, agosto de 1955, p. 11. Vide, também, MCCARTHY, John. Ascribing Mental Qualities to Machines, In:

do paralelo com o chamado "jogo da imitação", no qual um terceiro dialogando com duas outras pessoas escondidas, procura adivinhar, pelas perguntas e respostas, qual delas seria homem e qual seria mulher[6]. O exemplo do jogo foi tão didático que essa referência passou a ser conhecida pelo "teste de Turing", e vem sendo utilizado para avaliar a capacidade de um programa ou de uma máquina de apresentar comportamento inteligente. Ou seja: o teste mensura se e em quantas possíveis leituras da realidade a máquina é capaz de detectar, compreender, reagir e decidir em comparação a um ser humano e, até mesmo, se ela é capaz de enganar um ser humano, passando-se por outro.

Philosophical perspectives in artificial intelligence, RINGL, M (ed.), Atlantic Highlands, N.J.: Humanities Press, 1979, p. 02.

6 TURING, Alan M.. Computing Machinery and Intelligence, In: *Mind, A Quarterly Review of Psychology and Philosophy, New Series*, New York: Oxford University Press, vol. LIX, nº 236, outubro de 1950, pp. 433-460, p. 433-434. Nas palavras do próprio Turing, em tradução livre: "A nova forma do problema pode ser descrita nos termos de um jogo que denominamos de "jogo da imitação". Ele é jogado com três pessoas: um homem (A), uma mulher (B), e um interrogador (C) que pode ser de qualquer sexo. O interrogador fica numa sala separada dos outros dois. O objetivo do jogo para o interrogador é determinar qual dos dois outros é o homem e qual é a mulher. Ele os conhece pelos rótulos "X" e "Y" e, ao final do jogo, ele deve dizer "X é A e Y é B" ou "X é B e Y é A". Ao interrogador é autorizado colocar questões para A e B, assim: C: Será que X poderia, por favor, me dizer o comprimento de seu cabelo? Agora imagine que X realmente seja A, então A deve responder. É tarefa de A no jogo tentar fazer com que C promova uma identificação errônea. Sua resposta, então, pode ser: "Meu cabelo está coberto, e meus fios mais longos são de nove polegadas." Para evitar que o tom da voz auxilie o interrogador as respostas devem ser feitas por escrito, ou melhor ainda, datilografadas. O arranjo ideal é ter uma comunicação via 'teleprinter' entre as duas salas. Alternativamente, as perguntas e respostas podem ser repetidas por um intermediário. O objetivo do jogo para o terceiro jogador (B) é ajudar o interrogador. A melhor estratégia para ela é provavelmente dar respostas verdadeiras. Ela pode dizer coisas como "eu sou a mulher, não dê ouvidos a ele!" em suas respostas, mas isso não vai adiantar nada se o homem puder fazer afirmações semelhantes. Nós, então, formulamos a pergunta: "o que acontecerá quando a máquina tomar o lugar de A nesse jogo?" Será que o interrogador tomará as decisões erradas que tomou quando o jogo for jogado assim, em comparação com as que ele toma quando o jogo é jogado entre um homem e uma mulher?" Estas perguntas substituem nossa pergunta original: "as máquinas podem pensar?"

O certo, por ora, é que mesmo que uma máquina seja considerada "inteligente", é fundamental compreender qual o alcance dessa inteligência até para saber em quais setores e com qual grau de eficiência ela poderia ser empregada em pesquisas preditivas de decisões dos Tribunais em temas de processo penal.

Desde a divisão criada pelo filósofo John Searle em 1980, consagrou-se na doutrina em geral[7] a classificação do uso da inteligência artificial em "fraca" e "forte"[8]. A inteligência artificial chamada de "fraca", explica Searle, "nos dá ferramentas muito potentes", isto é, "nos permite formular e testar hipóteses de forma mais rigorosa e precisa"[9], porém, ela depende do inserção de conhecimento fornecido pelo ser humano que a programa, sendo que a máquina não é capaz de produzir raciocínios próprios, autônomos. Já na chamada inteligência artificial "forte", explica Searle, "o computador não é uma mera ferramenta no estudo da mente, ao contrário, o computador adequadamente preparado é realmente uma mente, no sentido de que os computadores que recebem os programas certos poderiam estar, literalmente, preparados para compreender e ter outros estados cognitivos"[10]. A inteligência "forte", portanto, seria aquela capaz de criar consciência, simulando raciocínios complexos e emitindo opiniões autônomas, independente da interferência constante do ser humano.

A viabilidade da inteligência artificial "forte", no entanto, foi objeto de acirrada crítica por parte de John Searle, valendo-se do exemplo

---

7 Vide, por todos: RUSSELL, Stuart; NORVIG, Peter. *Inteligência Artificial*, 3ª ed., tradução de Regina Célia Simille, Rio de Janeiro: Campus Elsevier, 2013, p. 1173.

8 SEARLE, John R.. Minds, Brains and Programs, In: *The Behavioral and Brain Sciences*, 3, Cambridge: Cambridge University Press, 1980, pp. 417-457, p. 417.

9 SEARLE, John R.. Minds, Brains and Programs, In: *The Behavioral and Brain Sciences*, 3, Cambridge: Cambridge University Press, 1980, pp. 417-457, p. 417. Tradução livre.

10 SEARLE, John R.. Minds, Brains and Programs, In: *The Behavioral and Brain Sciences*, 3, Cambridge: Cambridge University Press, 1980, pp. 417-457, p. 417. Tradução livre.

por ele denominado de "o quarto chinês"[11], para explicar sua posição. Searle se usa de exemplo imaginando que ele, que não sabe nada da língua chinesa, estaria trancado e isolado num quarto recebendo uma folha de papel na qual estão escritos ideogramas em chinês. Como não conhece a língua, não entende nada do que está escrito. Então, ele recebe uma segunda folha, na qual estão ideogramas chineses acompanhados de um conjunto de regras em inglês que permitem correlacionar a segunda folha com a primeira. E, finalmente, ele recebe uma terceira folha com ideogramas chineses, também com regras em inglês que o orientam a dar em resposta específicos ideogramas chineses vinculados a outros ideogramas da terceira folha, correlacionando os elementos desta terceira folha com as duas anteriores. Pessoas que ele não conhece e estão fora do quarto denominam a terceira folha de "script", a segunda folha de "história" e a primeira folha de "questões". Então, essas pessoas consideram que os símbolos que Searle entregou em resposta à terceira folha são chamados de "respostas às questões" e o conjunto de regras que lhe foi entregue é chamado de "o programa". Searle avança explicando que depois de um tempo ele fica muito bom em dar respostas seguindo as regras que permitem manipular os símbolos chineses e algo similar ocorre com os programadores do lado de fora do quarto, os quais ficam muito bons em escrever os programas de seu ponto de vista externo. Com isso, as respostas que Searle dá às questões se tornam indistinguíveis daquelas que um nativo da língua chinesa daria. Qualquer um que olhe suas respostas não diria que Searle não fala chinês. Sucede que se o mesmo experimento for feito com textos em inglês, língua nativa de Searle, ele daria respostas em patamares similares, igualmente corretas. Com esse experimento, o que Searle quer provar é que, no primeiro caso, em chinês, ele opera como um computador: até responde corretamente, mas não tem a menor ideia do que está respondendo. No segundo, em inglês, ele responde como um ser humano, isto é, sabe perfeitamente o que está respondendo, tem consciência do que responde. Enfim, Searle equipara o quarto ao computador e o ser humano falante de inglês e respondente em chinês ao "software" de inteligência artificial. Para Searle há uma limitação intransponível nessa

[11] SEARLE, John R.. Minds, Brains and Programs, In: *The Behavioral and Brain Sciences*, 3, Cambridge: Cambridge University Press, 1980, pp. 417-457, pp. 417 e ss..

conjuntura que impede sua compreensão do que está respondendo em chinês. Partindo desse exemplo, Searle acrescenta uma crítica ainda mais contundente à possibilidade de desenvolvimento da inteligência artificial "forte", dizendo que "a menos que você acredite que a mente é separável do cérebro, tanto conceitual quanto empiricamente – dualismo no sentido forte – você não pode esperar reproduzir a mentalidade escrevendo e rodando programas, já que programas precisam ser independentes do cérebro ou de qualquer outra forma particular de instanciação."

Assim, enquanto o computador responde de forma sintática, a mente humana responde de forma semântica e esta, explica Searle, envolve intencionalidade[12]. É certo que há visão contrária ao pensamento de Searle, sendo a mais incisiva aquela de Daniel Dannett[13]. De outro lado, também é certo que em decorrência do ainda não completo desenvolvimento da inteligência artificial "forte", havendo até mesmo, a partir da crítica de Searle[14], tanto algum ceticismo em relação à sua potencialidade de efetivação plena[15], quanto certo conservadorismo fundado no receio de ser ridicularizado e na preocupação em manter a "respeitabilidade" científica[16], a concentração da análise neste artigo focará na utilização da chamada inteligência artificial "fraca" no processo penal. Esse enfoque também se justifica na medida em que a inteligência artificial "fraca" é

---

12 SEARLE, John R.. *Intencionalidade*, tradução de Julio Fischer e Tomás R. Bueno. São Paulo: Martins Fontes, 2002, p. 365.

13 DENNETT, Daniel C.. *Darwin's Dangerous Idea*: evolution and the meaning of life. New York: Simon & Schuster Paperbacks, 1995, p. 445.

14 SEARLE, John R.. Minds, Brains and Programs, In: *The Behavioral and Brain Sciences*, 3, Cambridge: Cambridge University Press, 1980, pp. 417-457pp. 423-424. Tradução livre.

15 Vide, para além do texto original já citado de John Searle, dentre outros: MATHEWS, Eric. *Mente*: conceitos-chave em filosofia, tradução de Michele Tse, Porto Alegre: Artmed, 2007, pp. 96-97; e também: NILSSON, Nils J. *The Quest for Artificial Intelligence*: a history of ideas and achievements. New York: Cambridge University Press, 2009, p. 319; PRIMO, Alex; COELHO, Luciano. A chatterbot Cybelle: a experiência pioneira no Brasil, In: RAMOS, Roberto (org.) *Mídia, Textos e Contextos*. Porto Alegre: Edipucrs, 2001, pp. 259-276, p. 274.

16 BOSTROM, Nick. *Superinteligência*: caminhos, perigos e estratégias para um mundo novo. Tradução de Aurélio Antonio Monteiro, Clemente Genil Penna, Fabiana Geremias Monteiro, Patricia Ramos Geremias, Rio de Janeiro: Darkside Books, 2018, p. 48.

justamente aquela que vem sendo usada para estabelecer predições de decisões nos processos e ainda é muito cedo para imaginar programas de inteligência artificial que possam ir além, no sentido "forte" acima referido. Estabelecida esta limitação, antes de ingressar nos problemas de instrução da inteligência artificial "fraca", é preciso identificar como ela se organiza a partir dos algoritmos.

2. Algoritmos e dificuldades operacionais da inteligência artificial.

Como se vem referindo, não há como estabelecer uma análise crítica das potencialidades de uso da inteligência artificial na predição de decisões dos magistrados no processo penal se não houver mínima compreensão de como ela se estrutura e se organiza. E aqui entram em cena os algoritmos.

São os algoritmos que dão vida à máquina. Eles se caracterizam por um "conjunto de instruções matemáticas" ou "uma sequência de tarefas" que informam "ao computador o que ele deve fazer" "para alcançar um resultado esperado em um tempo limitado"[17]. Para tanto, os computadores requerem "instruções precisas e não ambíguas"[18]. Pedro Domingos ilustra que "os computadores são compostos por bilhões de minúsculas chaves chamadas transistores, e os algoritmos ligam e desligam essas chaves bilhões de vezes por segundo. O algoritmo mais simples é: gire a chave"[19].

Então, para que uma máquina possa ser capaz de passar no "teste de Turing", acima referido, e ser compreendida como dotada de "inteligência artificial", é preciso dotá-la de tantos algoritmos quantos sejam

---

[17] DOMINGOS, Pedro. *O Algoritmo Mestre*: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo, tradução de Aldir José Coelho Corrêa da Silva, São Paulo: Novatec, 2017, p. 24.

[18] KAUFMAN, Dora. *A Inteligência Artificial irá Suplantar a Inteligência Humana?* Barueri, SP: Estação das Letras e Cores, 2018, *passim*.

[19] DOMINGOS, Pedro. *O Algoritmo Mestre*: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo, tradução de Aldir José Coelho Corrêa da Silva, São Paulo: Novatec, 2017, p. 24.

necessários para "ensinar" a máquina, fazendo-a ter a representação do conhecimento e ser capaz de ultrapassar a barreira do idioma natural[20].

A representação do conhecimento é o ato de descrever um conhecimento, em pedaços, para que a inteligência artificial "assimile" onde e como deverá aplicar tal informação, baseando-se em experiências anteriores. Quando se fala em "conhecimento", portanto, se refere à informação que um "software" precisa para apresentar um comportamento considerado inteligente. Com a aquisição de conhecimento é possível construir o que se denomina de "sistema especialista", isto é, "um programa acoplado a um banco de memória que contém conhecimentos sobre uma determinada especialidade"[21].

Já a tarefa de vencer a barreira do idioma natural e identificar novas referências linguísticas utilizadas, sejam faladas ou escritas, é mais difícil para a inteligência artificial, pois uma mesma palavra, a depender do contexto, pode ter significados distintos. Para ilustrar a complexidade do que isso representa, aqui calha a lição do "segundo"[22] Wittgenstein ao explicar que quando o ser humano ouve uma palavra, paira-lhe "no espírito a mesma coisa, e que o seu emprego pode ser um outro"[23], isto é, pode ter significados diferentes em ocasiões diferentes. Em sentido similar a lição de Warat ao explicar que "a mensagem nunca se esgota na significação de base das palavras empregadas. O sentido gira em torno do dito e do calado. Desta forma, o êxito de uma comunicação depende de como o receptor possa interpretar o sentido latente"[24]. Isso tudo con-

---

[20] DEBESSONET, Cary G.; CROSS, George R. . *An Artificial Intelligence Application in the Law: CCLIPS, a Computer Program That Processes Legal Information*. In: *High Technology Law Journal*, Vol. 1, Issue 2, Fall, 1987, pp. 329 e ss.

[21] FERNANDES TEIXEIRA, João de. *Mentes e Máquinas*, Porto Alegre: Artes Médicas, 1998, p. 53.

[22] Como é notório, estudiosos de Wittgenstein levam em conta que o filósofo mudou completamente sua forma de compreender a linguagem ao longo da vida e, assim, costumam dividir sua obra em dois momentos distintos, referindo-se ao "primeiro" e ao "segundo" Wittgenstein.

[23] WITTGENSTEIN, Ludwig. *Investigações Filosóficas*. 6ª ed., tradução de Marcos G. Nontagnoli, Petrópolis: Vozes, 2009, p. 81.

[24] WARAT, Luis Alberto. *O Direito e sua Linguagem*, 2ª ed., Porto Alegre: Sérgio Antonio Fabris Editor, 1995, p. 65.

duz à conclusão de que nos jogos de linguagem "a palavra deve ter uma família de significados"[25].

O que costuma acontecer com a máquina é que ela é "treinada" para ter uma determinada reação frente a tal signo, porém, levando em conta a possibilidade de um significado novo a partir do contexto, resta clara a enorme dificuldade de promover alguns avanços tecnológicos. A ferramenta que tem sido utilizada para a otimização dessa adaptação da máquina com as variações de significados dos signos linguísticos é a interação da inteligência artificial, com simulação de diálogos[26]. Quanto mais os "softwares" possam ser programados para desenvolver habilidade na troca informações com o ser humano em linguagem natural, maior será sua interação[27].

Isso tudo representa igual desafio quando se trata de alimentar uma inteligência artificial capaz de fazer as predições de decisões de juízes a partir da leitura e interpretação de decisões anteriores.

3. Paradigmas filosóficos estruturantes do conhecimento.

Nessa questão toda do ensinamento da máquina parece fundamental compreender que, se é possível ensinar uma máquina a pensar, é porque a estrutura do pensamento é capaz de ser reproduzida e aprendida. E aí é necessário remontar à forma paradigmática pela qual se estrutura o pensamento e o conhecimento humano.

Ao longo da história da humanidade são basicamente três os grandes paradigmas estruturantes do conhecimento: a metafísica clássica aristotélica que está em busca de uma essência e trabalha com a ideia

---

[25] WITTGENSTEIN, Ludwig. *Investigações Filosóficas*. 6ª ed., tradução de Marcos G. Nontagnoli, Petrópolis: Vozes, 2009, p. 57.

[26] PRIMO, Alex; COELHO, Luciano Roth. Comunicação e inteligência artificial: interagindo com a robô de conversação Cybelle. In: MOTTA, L. G. M. et al. (Eds.). *Estratégias e culturas da comunicação*. Brasília: Editora Universidade de Brasília, 2002. p. 83-106.

[27] AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi. *Máquinas Preditivas*: a simples economia da inteligência artificial, tradução de Wendy Campos, Rio de Janeiro: Alta Books, 2018, p. 01.

de verdade por correspondência[28]; a filosofia da consciência cartesiana, que separa corpo e alma, "fundando" um sujeito solipsista que sozinho diz o mundo a partir de si[29]; e a filosofia da linguagem, que altera a compreensão de uma relação sujeito-objeto para sujeito-sujeito, usando da linguagem intersubjetivamente construída como condição de possibilidade de compreensão do mundo[30].

Em que pese sejam formas diferentes de fundamentar a compreensão, todas as três influenciam a humanidade ocidental ainda hoje, operando de forma distinta, de pessoa para pessoa. Assim, é possível dizer que tanto quanto existem pessoas com predominâncias diferentes entre os paradigmas referidos, existem juízes que se comportam em igual disparidade. Portanto, existem juízes que são orientados pela ideia de busca da verdade real e saem atrás das provas que estão no mundo (fundados no paradigma da filosofia aristotélica, de uma verdade por correspondência que não está em mim, mas no mundo); outros que acreditam trazer a verdade dentro de si, desconsiderando as teses e manifestações das partes, e, por vezes, até mesmo a jurisprudência dominante ou a doutrina consagrada, para decidir "de acordo com a sua consciência" (fundados na filosofia da consciência que estrutura um sujeito solipsista, que sozinho diz o mundo a partir de si); e juízes que compreendem a importância da inércia jurisdicional compatibilizada com as garantias do contraditório e da ampla defesa, construindo uma decisão dialogada e intersubjetiva (fundados na intersubjetividade da filosofia da linguagem).

Não obstante os três modelos se apresentem no contexto dos seres humanos, por uma limitação própria das máquinas que ainda estão centradas no modelo da inteligência artificial "fraca", isto é, ainda não possuem "consciência", sua estruturação se organiza a partir do

---

[28] ARISTÓTELES. *Metafisica*. 2ª ed., tradução de Edson Bini, São Paulo: EDIPRO, 2012, pp. 177-178, 1027b24-1028ª2.

[29] DESCARTES, René. O Discurso do Método. In: *Descartes: obras escolhidas*. Organizadores: J. Guinsburg, Roberto Romano e Newton Cunha. Tradução de J. Guinsburg, Bento Prado Jr., Newton Cunha e Gita K. Guinsburg. São Paulo: Perspectiva, 2010, pp. 75 e 76; 87 e 88.

[30] HEIDEGGER, Martin. *Ser e Tempo*. 2ª ed., tradução de Márcia Sá Cavalcante Schuback, Petrópolis: Vozes, 2007, pp. 206 e ss. e pp. 209 e ss..

paradigma da filosofia clássica aristotélica de busca de uma verdade por correspondência.

Isso tudo compreendido, é possível avançar para refletir em torno dos limites envolvendo a construção dos algoritmos e as influências negativas que o paradigma aristotélico orientado por silogismos possa apresentar.

4. Algoritmos e os silogismos aristotélicos.

Como refere G.L. Simons, é inevitável aos que trabalham na área da inteligência artificial precisar escrutinar a inteligência natural, a fim de identificar "as características-chave, atributos definitivos, etc."[31]. Trilhando percurso similar, Roberto Vilhena recorda que os algoritmos acabam sendo estruturados nos moldes silogísticos desenhados por Aristóteles[32]. Essa percepção é fácil de assimilar, dado que a humanidade ocidental é primitivamente herdeira dessa estrutura do pensamento lógico e silogístico aristotélico. Também é interessante considerar que, etimologicamente, a palavra silogismo significa "com cálculo", o que denota, desde logo, como esse método é adaptável ao ensinamento da máquina que se vale igualmente de cálculos.

A inteligência artificial, então, utiliza-se de silogismos para imitar a compreensão de algum objeto, ou seja, realiza uma "operação intelectual" que visa alcançar todas as possibilidades de raciocínio. E estes silogismos são construídos através de redes de algoritmos (ou "diagramas de fluxo") introduzidos na máquina. Ao tratar do tema, Jordi Nieva Fenoll ilustra a construção destes diagramas de fluxo com um exemplo básico, porém esclarecedor, de como a máquina é ensinada a encontrar uma solução[33]: "Tenho fome. Opção 1: Tenho dinheiro: Subopção A: Compro comida. Subopção B: Poupo e jejuo. Opção 2: Não tenho dinheiro: Subopção

---

[31] SIMONS, G. L.. *Introdução à Inteligência Artificial*, tradução de Guilherme M. G. Dias Pires, Lisboa: Clássica Editora, 1986, p. 21.

[32] VILHENA, Roberto. O seu futuro depende do passado, In: *Casa do Saber*, 2019, *passim*.

[33] NIEVA FENOLL, Jordi. *Inteligencia artificial y proceso judicial*. Madrid: Marcial Pons, 2018, p. 21.

A: Jejuo.Subopção B: Roubo comida." O algoritmo, enfim, retomando a referência de Vilhena, está mais preocupado com a forma do pensamento, com sua estrutura, do que propriamente com o conteúdo. Não que o conteúdo não seja importante, mas, sabendo como o pensamento se estrutura, o algoritmo é capaz de substituir o ser humano. Não à toa, portanto, Simons conclui que "o uso de representações baseadas na lógica tornou-se popular na investigação de inteligência artificial (IA), porque estas ofereciam uma forma simples de derivação de novos factos a partir de factos velhos"[34].

É interesse compreender isso, pois, se a organização do método silogístico é empregada na inteligência artificial; se ela remete a Aristóteles; e se esse método influencia a humanidade ocidental ainda hoje, é importante compreender como esse pensamento silogístico opera, para ter presente a dimensão de utilização dos algoritmos e saber identificar os riscos que a estrutura silogística conduz. Somente assim se poderão identificar possíveis limitações na estruturação dos programas de inteligência artificial "fraca", visando evitar um uso dissociado da base democrática exigida para o processo penal.

Para tanto, inicia-se ponderando que o silogismo aristotélico pode ser lido em quatro vertentes (silogismo científico, dialético, poético e retórico). De todas essas possibilidades, no entanto, apenas a primeira, denominada pelo próprio Aristóteles de "silogismo científico", serve para a inteligência artificial "fraca", pois utiliza a dedução, a argumentação lógica e, no campo da inteligência artificial, pode ser vista como a análise de algoritmos realizada por "softwares". Esse silogismo científico trabalha com alto grau de previsibilidade, permitindo saber, dada uma determinada configuração algorítmica, qual resultado será alcançado[35]. Nessa linha metodológica muitos autores atribuem o seguinte exemplo de silogismo a Aristóteles: "Todo homem é mortal. Sócrates é um homem. Logo, Sócrates é mortal"[36].

---

[34] SIMONS, G. L. *Introdução à Inteligência Artificial*, tradução de Guilherme M. G. Dias Pires, Lisboa: Clássica Editora, 1986, p. 123.

[35] ARISTÓTELES. Analíticos Posteriores. In: *Órganon*, 2ª ed., tradução de Edson Bini, São Paulo: Edipro, 2010, Livro I, §2, 71b18, pp. 253-254.

[36] Como refere GUIMARÃES, Rodrigo Régnier Chemim. *Atividade Probatória Complementar do Juiz como Ampliação da Efetividade do Contraditório e da*

Na análise das decisões de juízes, orientada pela construção preditiva, após as reunir em grupo e as catalogar conforme seu teor, a inteligência artificial visa deduzir qual será o futuro entendimento de um juiz ou tribunal em relação a determinada situação. Se essa é a pretensão, e se o uso de silogismos científicos está na base na construção algorítmica, é certo que há uma limitação aqui, até porque a inteligência artificial, mesmo com os dados disponíveis, não poderá chegar sozinha a um entendimento próprio sobre a mesma situação, pois ela ainda não é capaz de produzir uma opinião original. Entra em cena, então, na construção do sistema analítico da máquina, a relação entre dois atores fundamentais: o engenheiro do conhecimento e o perito.

5. Potenciais entimemas na elaboração de sistemas peritos: um problema a ser considerado no emprego da inteligência artificial em análises preditivas.

Para que se possa desenvolver uma inteligência artificial capaz de ser aplicada ao processo penal com alguma utilidade, será necessário contar com a cooperação entre um engenheiro do conhecimento[37], isto é, aquele profissional encarregado de promover a programação heurística que instruirá a máquina e a fará "inteligente", e um perito.

O engenheiro do conhecimento e o perito dialogam na elaboração de um sistema perito capaz de ser empregado para solução de uma determinada questão prática. O engenheiro do conhecimento deve "mergulhar" no universo do perito, promovendo entrevistas e trocando impressões

Ampla Defesa no Novo Processo Penal Brasileiro. Tese, Curitiba: Universidade Federal do Paraná, 2017, p. 35: "No entanto, não há nenhuma passagem na obra de Aristóteles que utilize o referido exemplo e este, então, parece mais uma forma consagrada pela tradição de exemplificar o silogismo aristotélico. Jan Lukasiewicz informa que uma variação desse famoso exemplo, com referência a "animal" ao invés de "mortal", encontra-se em texto de Sexto Empírico (160 a. C.). Aristóteles, por sua vez, dá exemplos menos "poéticos": "Se A se aplica a B, e B a C, A se aplica a C"; ou, então: "Pitaco é liberal, porque aqueles que prezam a honra são liberais e Pitaco preza a honra""

37 FERNÁNDEZ, Gregorio. Panoramas de los sistemas expertos. In: CUENA, José (org.) *Inteligencia Artificial*: sistemas expertos. Madrid: Alianza Editorial, 1986, pp. 23-52, p. 38.

com o intuito de reduzir a complexidade do campo específico do conhecimento às questões centrais que são necessárias para a máquina realizar determinada tarefa. Ele deve, enfim, "persuadir o perito a traduzir a sua perícia numa forma que possa ser armazenada numa base de dados"[38]. E aqui se estabelecem alguns perigos quando se pensa em programação voltada para o processo penal.

O primeiro perigo reside tanto na incapacidade do perito escolhido para servir de ponte com o conhecimento específico do processo penal, quanto na incapacidade de tradução dos aspectos relevantes do direito e do processo penal pelo engenheiro do conhecimento. Não é preciso muito esforço para identificar na doutrina de processo penal de hoje em dia uma pluralidade bastante significativa de discursos e fundamentos antagônicos.

Esse tipo de problema não é uma exclusividade do processo penal, por óbvio, sendo mesmo uma preocupação geral quando se trata de elaborar sistemas peritos[39]. No entanto, no processo penal ele é significativamente marcante, dada a variedade de visões coexistentes na doutrina. Por exemplo: se o perito for um doutrinador mais "tradicional" ele é capaz dele indicar que a função do juiz no processo penal seja a "busca da verdade real". Porém, se for um doutrinador mais "moderno", isto é, que faça leituras transdisciplinares[40] da complexidade do processo penal e premie leituras e filtragens constitucionais das regras processuais, ele refutará essa ideia como ponto de partida. Aliás, mesmo entre os doutrinadores mais "modernos" há ampla disparidade a respeito de qual seja o papel do juiz nessa questão, indo da inércia absoluta[41] até

---

[38] SIMONS, G. L. *Introdução à Inteligência Artificial*, tradução de Guilherme M. G. Dias Pires, Lisboa: Clássica Editora, 1986, p. 112.

[39] FERNÁNDEZ, Gregorio. Panoramas de los sistemas expertos. In: CUENA, José (org.) *Inteligencia Artificial: sistemas expertos*. Madrid: Alianza Editorial, 1986, pp. 23-52, p. 45.

[40] Como refere COUTINHO, Jacinto Nelson de Miranda. Dogmática Crítica e Limites Linguísticos da Lei. In: *Diálogos Constitucionais: direito, neoliberalismo e desenvolvimento em países periféricos*. COUTINHO, Jacinto Nelson de Miranda; LIMA, Martonio Mont'Alverne Barreto (Organizadores). Rio de Janeiro: Renovar, 2006, pp. 225-232, p. 227.

[41] *V.g.* KHALED JR., Salah H. *A busca da verdade no processo penal*: para além da ambição inquisitorial. São Paulo: Atlas, 2013, p. 151; BARROS, Flaviane

a compatibilização com posturas ativas na produção da prova[42]. Essa mesma disparidade doutrinária se reproduz no comportamento e na exegese dos juízes criminais. Ao se conduzir uma pesquisa em torno do modo decisório dos juízes e dos tribunais, portanto, seria importante, no mínimo, deixar clara a opção que embasa a construção do sistema perito e que alimentará a inteligência artificial.

O segundo perigo decorre da necessidade do engenheiro do conhecimento "decidir qual das várias estruturas de resolução de problemas ('procedimentos de inferência") é a mais adequada para o assunto específico"[43]. Em verdade, esse é um esforço de contínuo aperfeiçoamento que deve nortear a elaboração de qualquer sistema perito. Como recorda G. L. Simons, "os programadores deverão ter por objectivo produzir o primeiro esboço do sistema tão rapidamente quanto possível, se não por outra razão, para conservar o interesse do perito". E complementa dizendo que "é provável que ocorram erros na primeira versão, e o envolvimento do perito será essencial para que ela seja melhorada. É nessa altura que as inconsistências nos conhecimentos do perito, ou a sua compreensão superficial dos seus vários métodos de resolução efectiva de problemas, são provavelmente expostas"[44].

Retoma-se aqui o problema do emprego de algoritmos na elaboração de uma inteligência artificial. Se ele parte de um silogismo científico,

---

de Magalhães. *(Re)forma do Processo Penal*: comentários críticos dos artigos modificados pelas leis n. 11.690/08 e 11.719/08. Belo Horizonte: Del Rey, 2009, pp. 50-51; TASSE, Adel El; MILÉO, Eduardo Zanoncini; PIASECKI, Patrícia Regina. *O Novo Sistema de Provas no Processo Penal. Comentários à Lei 11.690/08*. Curitiba: Juruá, 2008, p. 65.

42 Admitindo, por exemplo, que o juiz possa ao menos complementar a inquirição das testemunhas nos moldes hoje permitidos pelo art. 212 do Código de Processo Penal: *v.g.* COUTINHO, Jacinto Nelson de Miranda. Sistema Acusatório e Outras Questões Sobre a Reforma Global do CPP. In: COUTINHO, Jacinto Nelson de Miranda e CARVALHO, Luis Gustavo Grandinetti Castanho (Organizadores) *O Novo Processo Penal à Luz da Constituição*. Volume 2. Rio de Janeiro: Lumen Iuris, 2011, pp. 20-21; LOPES JR., Aury. *Direito Processual Penal*. 10ª ed., São Paulo: Saraiva, 2013, p. 657.

43 SIMONS, G. L. *Introdução à Inteligência Artificial*, tradução de Guilherme M. G. Dias Pires, Lisboa: Clássica Editora, 1986, p. 113.

44 SIMONS, G. L. *Introdução à Inteligência Artificial*, tradução de Guilherme M. G. Dias Pires, Lisboa: Clássica Editora, 1986, p. 113.

como acima destacado, pode ocorrer algo equivalente ao problema que o próprio Aristóteles alertava para a adequada elaboração de um silogismo: não atentar para a necessidade de que a premissa maior seja verdadeira. Aqui se corre o risco de um engenheiro do conhecimento ou um programador ensinarem a máquina de forma errada, isto é, partindo de um entimema. Como explica Aristóteles, o "entimema [é] formado de poucas premissas e em geral menos do que o silogismo primário", "porque se alguma dessas premissas for bem conhecida, nem sequer é necessário enunciá-la; pois o próprio ouvinte a supre".[45]

Se o entimema é formado uma premissa maior dada como certa[46], é preciso entender que esta, por sua vez, pode estar se originando de um preconceito, o qual pode ser até mesmo indemonstrável, quiçá originário do inconsciente, e pode estar presente, seja no perito por ocasião da orientação ao engenheiro que ensinará a máquina, seja no juiz cujas decisões anteriores serão analisadas pela inteligência artificial para elaborar a predição.

É, portanto, na interseção entre a filosofia e a psicanálise, e na presença do silogismo que embasa a inteligência artificial que a construção do entimema e a análise preditiva ganham complexidade. Tudo isso casa com a preocupação do filósofo francês Eric Sadin, destacada no documento da Comissão Europeia para a Eficácia da Justiça, de dizer que a ideia de "neutralidade" dos algoritmos é um mito[47]. Talvez isso tudo explique os dois caminhos que vêm sendo trilhados quanto à possibilidade de se admitir o uso da inteligência artificial na elaboração de predições das decisões judiciais e sirva de alerta para que se tenha maior

---

45 ARISTÓTELES. *Retórica*. Tradução de Edson Bini, São Paulo: Edipro, 2011, I, 1357a.

46 Como detalha ADEODATO, João Maurício. *Ética e Retórica*: para uma teoria da dogmática jurídica, 5ª ed., São Paulo: Saraiva, 2012, p. 302: "Aristóteles junta os *topoi* que servem para fundamentar os entimemas, sejam reais ou aparentes: o emprego de oposições e equivalências de termos (antônimos e sinônimos), a comparação, diferenças de grau, experiências anteriores, polissemias, ambiguidades, juízos de valor generalizados. Ele enumera vinte e oito desses pontos de vista, fornecendo exemplos de *topoi* construindo entimemas."

47 EUROPA. Conselho da Europa. Comissão Europeia para a Eficácia da Justiça, *Carta Ética Europeia de Utilização da Inteligência Artificial nos Sistemas Judiciários e seu Entorno*, Estrasburgo: CEPEJ, 03 de dezembro de 2018, p. 61.

cuidado na construção dos sistemas peritos que nortearão as pesquisas preditivas daqui em diante.

6. O modelo de pesquisa norte-americano.

Em 2017 os pesquisadores norte-americanos Daniel Martin Katz, Michael J. Bommarito e Josh Blockman fizeram um experimento com a Suprema Corte daquele país utilizando um "software" capaz de prever votos em processos. Realizaram uma análise dos julgados de dois séculos daquela Corte, acertando 70,2% dos resultados dos julgados e 71,9% dos votos dos juízes[48]. Estabeleceram a possibilidade de decisões serem previstas por inteligência artificial, utilizando os parâmetros dos próprios juízes. Levaram em conta três outras pesquisas anteriores (realizadas entre 2004 e 2011), que haviam alcançado resultados limitados e questionáveis, decorrência do quanto de dados eram inseridos no sistema[49]. Nas pesquisas anteriores a análise era limitada à composição plena da Suprema Corte e se circunscrevia ao momento anterior à mudança de algum de seus integrantes. A última pesquisa teve a pretensão de utilizar a inteligência artificial que fosse capaz de manter as previsões, mesmo com a alteração de magistrados ao longo dos anos.

Como insumos para alimentar a inteligência artificial os pesquisadores utilizaram o Banco de Dados da Suprema Corte (SCDB) e "alguns recursos derivados da engenharia de recursos"[50], não deixando claro quais seriam estes últimos.

---

48 KATZ, Daniel Martin; BOMMARITO, Michael J.; BLOCKMAN, Josh. A general approach for predicting the behavior of the Supreme Court of the United States, In: *PLoS ONE*, 12(4): e0174698, 2017, *passim*.

49 MARTIN, A. D.; QUINN, K.M.; RUGER, T.W.; KIM, P.T.. Competing approaches to predicting supreme court decision making, In: *Perspectives on Politics*, 2004; 2(4), pp. 761–767; e também GUIMERÀ, R., SALES-PARDO, M.. Justice blocks and predictability of us supreme court votes. In: *PloS One*, 2011; 6(11):e27188. pmid:22096533; e, ainda, RUGER, T. W.; KIM, P. T.; MARTIN, A. D.; QUINN, K. M.. The supreme court forecasting project: Legal and political science approaches to predicting supreme court decisionmaking, In: *Columbia Law Review*, New York: Columbia Law School, 2004; 104(4), pp. 1150–1209.

50 KATZ, Daniel Martin; BOMMARITO, Michael J.; BLOCKMAN, Josh. A general approach for predicting the behavior of the Supreme Court of the United

Quanto ao que inferiram do banco de dados referido os pesquisadores relataram algumas dificuldades interessantes. Disseram que uma delas residiu, por exemplo, no fato de que a Suprema Corte norte-americana por vezes julga pressionada pela opinião pública, ou influenciada pelo conflito entre agências estatais, a ponto de invocarem uma máxima por lá consagrada: "desempenho passado não necessariamente prediz resultados futuros".

Relataram, também, dificuldades em compatibilizar a pesquisa com a mudança jurisprudencial repentina, que esvazia as referências anteriores na predição futura. Seguiram aduzindo que outra dificuldade se relaciona com o fato de que em cada decisão encontraram "até duzentos e quarenta variáveis, incluindo variáveis cronológicas, variáveis de fundo de caso, variáveis específicas de Justiça e variáveis de resultado. Muitas dessas variáveis são categóricas, assumindo centenas de valores possíveis. Por exemplo, a variável de problema pode ter 384 valores distintos".

Tentaram, então, estabelecer alguns parâmetros padronizados para a pesquisa, criando um mapa de codificação que definia uma coluna para os votos singulares e outra para a decisão final do colegiado. Os votos e a decisão da Corte eram catalogados como "reversos" (quando eram pela mudança da decisão da Corte inferior); "afirmativos" (quando se decidiam por manter a decisão recorrida) e "outros" (quando a decisão caminhava para uma solução diversa, por exemplo, perda de objeto).

Depois relacionaram as referências utilizadas no SCDB: qual ministro, qual o mandato do ministro, juiz natural, mês de discussão, requerente, requerido, competência originária ou recursal, ações administrativas, tribunal de origem, fonte do caso, desacordo de primeira instância, motivo para decidir pela análise do caso na Suprema Corte, decisão da primeira instância, composição do tribunal de origem e qual era o tema.

Acrescentaram variáveis dos tribunais inferiores identificando que, a depender do tribunal de origem, a decisão da Suprema Corte era tendente a ser num sentido. Em seguida adicionaram novos dados: se houve ou não sustentação oral; se houve mais de uma sessão de julgamento; o tempo de discussão do caso. O tempo, perceberam os pesquisadores, influencia na decisão ser unânime ou não.

States, In*: PLoS ONE*, 12(4): e0174698, 2017, *passim*.

Por fim, desenvolveram recursos que resumiam o "comportamento" de um juiz ou tribunal de primeira instância e a diferença entre eles, dividindo essas características em três categorias: (1) características relacionadas à taxa de reversão; (2) características relacionadas à orientação política da decisão, se de esquerda ou de direita; e (3) características relacionadas à taxa de dissidência. Incluíram, ainda, um termo de diferença entre a decisão de primeira instância e decisão média historicamente observada, o que permitiu identificar o quão distante, ideologicamente, estava a opinião do juiz de primeira instância em comparação com o ministro da Suprema Corte, revelando tendências políticas e processuais dos Tribunais e dos juízes.

Os pesquisadores ainda indicaram que se utilizaram do chamado "algoritmo da floresta aleatória" ("random forest"). Este algoritmo é de aprendizagem supervisionada e cria combinações de árvores de decisão[51].

Este modelo norte-americano de pesquisa livre, predominante naquele país, então, como se vê da explicação da última experiência realizada, é bastante complexo e necessitou da contribuição das referidas pesquisas anteriores para identificar e corrigir algumas falhas. A tendência é que com o tempo novas pesquisas avancem ainda mais. Não há notícia de reação negativa institucional por parte da Suprema Corte daquele país, nem tampouco que o Congresso norte-americano esteja pensando em regrar a análise preditiva de julgados, o que indica que não há regulamentação cerceadora da atividade de pesquisa empírica que possa predizer o modo de julgar dos tribunais norte-americanos.

---

[51] Niklas Donges apresenta uma analogia facilitadora para compreender o algoritmo da floresta aleatória: "Andrew quer decidir para onde viajar em suas férias de um ano, então ele pede sugestões para as pessoas que mais bem o conhecem. O primeiro amigo que ele encontra lhe pergunta a respeito do que ele gostou e do que não gostou em suas viagens anteriores. Baseado nestas respostas, ele dá algumas sugestões a Andrew. Esta é uma abordagem típica de árvores de decisão. O amigo de Andrew criou regras para guiar sua decisão sobre o que deveria recomendar, usando para tanto as respostas de Andrew. Depois disto, Andrew começa a pedir conselhos para mais e mais amigos e eles novamente fazem diferentes perguntas das quais eles conseguem extrair algumas recomendações. Finalmente, Andrew escolhe os lugares que receberam mais recomendações, o que é uma abordagem típica de florestas aleatórias." (DONGES, Niklas. A Complete Guide to the Random Forest Algorithm. In: *Built In*, 16 de junho de 2019).

7. A reação francesa.

Na França a situação é totalmente oposta àquela norte-americana. O Poder Legislativo francês aprovou, no dia 23 de março de 2019, a Lei 2019-222, alterando o artigo L10 do Código de Justiça Administrativa francês para alcançar o extremo de criminalizar a conduta de quem "divulga os dados de identidade dos magistrados e membros do registro" que "não podem ser objeto de reutilização com a finalidade ou efeito de avaliar, analisar, comparar ou prever suas práticas profissionais reais ou alegadas"[52], punida com uma pena máxima de 5 (cinco) anos.

O mais curioso é que a lei foi precedida de uma decisão do Conselho Constitucional francês ("Conseil constitutionnel")[53], que é um colegiado de nove membros com jurisdição para analisar a constitucionalidade das leis, inclusive "ex ante", como neste caso. Na análise do caso, o Conselho Constitucional francês refere aos argumentos de alguns deputados que levaram o caso até ele, os quais contestavam a regra que impunha o sigilo e a proibição de conhecimento dos nomes dos juízes e da sua jurisprudência, aduzindo que o conhecimento destes favoreceria a igualdade entre os litigantes. As críticas também foram feitas por outros deputados e senadores, ao argumento central de ferimento do princípio da publicidade.

O Conselho, por sua vez, ponderou que "o legislador pretendia evitar que a reutilização dos nomes e decisões dos juízes permitisse, por meio de processamento de dados pessoais, traçar o perfil dos profissionais da área jurídica com base nas decisões tomadas, o que poderia levar à pressão ou escolha de estratégias de jurisdição ou alterar o funcionamento da Justiça"[54]. E seguiu ponderando que "estas disposições não criam, portanto, qualquer disfunção injustificada entre litigantes e não infringem o direito a um procedimento justo e equitativo que garanta o equilíbrio dos direitos das partes"[55]. E, assim, concluíram pela constitucionalidade

---

[52] FRANÇA. *Lei 2019-222, de 23 de março de 219*. Artigo 33.

[53] FRANÇA. Conseil Constitucionnel. *Décision nº 2019-778 DC du 21 mars 2019*.

[54] FRANÇA. Conseil Constitucionnel. *Décision nº 2019-778 DC du 21 mars 2019*, parágrafo 93. Tradução livre.

[55] FRANÇA. Conseil Constitucionnel. *Décision nº 2019-778 DC du 21 mars 2019*, parágrafo 94. Tradução livre.

da criação do tipo penal referido, dando carta branca ao Parlamento para seguir na edição da referida lei.

Ao criminalizar pesquisas sobre os julgados, o novo regramento francês indica caminhar no sentido oposto à tradição iluminista de considerar a publicidade como garantia, insculpida, a partir da Revolução Francesa, inclusive e em certa medida, até mesmo na Declaração Universal dos Direitos do Homem e do Cidadão, de 1789. Com efeito, ainda que o Conselho francês tenha afirmado em sentido inverso, fixando sua análise nos artigos 6º e 16 da Declaração, olvidou do artigo 15 do mesmo histórico diploma normativo. Este estabelece que "a sociedade tem o direito de pedir contas a todo agente público pela sua administração", de onde decorre o dever de "accountability", isto é, de prestação de contas, e, por conseguinte, de publicidade dos atos do poder público, aqui incluindo, por evidente, as decisões dos juízes.

8. O ponto de equilíbrio da Comissão Europeia para a Eficácia da Justiça – CEPEJ: entre a filosofia crítica de Eric Sadin e o otimismo matemático de Cristian Calude e Giuseppe Longo.

Os dois extremos evidenciados entre o que se produz nos Estados Unidos e a proibição criminalizadora da legislação francesa parecem escapar do quanto vem sendo trabalhado no âmbito da comunidade europeia em torno do tema da tecnologia da informação e comunicação dos sistemas europeus de Justiça.

Em sua 31ª reunião plenária realizada nos dias 03 e 04 de novembro de 2018, a Comissão Europeia para a Eficácia da Justiça ("Commission européenne pour l'efficacité de la justice – CEPEJ") editou uma "Carta Ética Europeia de Utilização da Inteligência Artificial nos Sistemas Judiciários e seu Entorno"[56]. Nela se evidencia certo receio da Comissão Europeia quanto ao uso da inteligência artificial, mas a Carta Ética está longe de proibir o emprego da tecnologia e, mesmo muito distante da iniciativa francesa de tipificar pesquisas preditivas de jurisprudência como crime.

[56] EUROPA. Conselho da Europa. Comissão Europeia para a Eficácia da Justiça. *Carta Ética Europeia de Utilização da Inteligência Artificial nos Sistemas Judiciários e seu Entorno*, Estrasburgo: CEPEJ, 03 de dezembro de 2018.

A Comissão Europeia faz, no entanto, algumas ressalvas, dizendo que "o termo "justiça preditiva" deve ser refutado porque é ambíguo e falacioso" e que "os vieses de análise, se eles não podem ser totalmente excluídos, devem ser identificados"[57]. Seja como for, em geral, ainda que a Carta Europeia externe certa preocupação, ela não proíbe, de partida, a análise de decisões judiciais e a estruturação de mecanismos de inteligência artificial que possam ser preditivos.

Aliás, na 32ª e última reunião plenária realizada pela Comissão Europeia para a Eficácia da Justiça, em 14 de junho de 2019 (posterior à edição da lei francesa, portanto), elaborou-se um documento denominado "Caixa de ferramentas para apoiar a implantação das Diretrizes na condução da mudança para a ciberjustiça", no qual se registram recomendações no sentido de facilitar a supervisão dos tribunais e do Ministério Público, bem como garantir a transparência, inclusive no sentido de combater a corrupção e oferecer um "sistema razoavelmente previsível"[58].

Nesse campo, portanto, a lei francesa caminha contra a tendência externada nas reuniões plenárias e nas diretrizes europeias recomendadas pela Comissão Europeia para a Eficácia da Justiça, do Conselho da Europa. Enquanto na Comissão Europeia não há vedação para as pesquisas preditivas, na França a conduta é criminalizada.

Uma das maiores preocupações da Comissão Europeia, no entanto, vem na trilha do alerta de Eric Sadin ao dizer que a ideia de "neutralidade" dos algoritmos é um mito[59]. Aqui transparece um ponto de inflexão entre o modelo liberal norte-americano e o modelo proibicionista francês. Essa preocupação de Eric Sadin se revela importante, notadamente quando se toma como séria a possibilidade da instrução da máquina de inteligência artificial ser organizada a partir de possíveis entimemas que possam ser

---

[57] EUROPA. Conselho da Europa. Comissão Europeia para a Eficácia da Justiça. *Carta Ética Europeia de Utilização da Inteligência Artificial nos Sistemas Judiciários e seu Entorno*, Estrasburgo: CEPEJ, 03 de dezembro de 2018, p. 61.

[58] EUROPA. Conselho da Europa. Comissão Europeia para a Eficácia da Justiça, *Boîte à outils pour soutenir la mise en œuvre des Lignes Directrices sur la conduite du changement vers la cyberjustice*, Estrasburgo: CEPEJ, 13-14 de junho de 2019, pp. 14-15.

[59] EUROPA. Conselho da Europa. Comissão Europeia para a Eficácia da Justiça, *Carta Ética Europeia de Utilização da Inteligência Artificial nos Sistemas Judiciários e seu Entorno*, Estrasburgo: CEPEJ, 03 de dezembro de 2018, p. 61.

o norte da pesquisa ou mesmo na dificuldade de conduzir uma pesquisa quando há ampla disparidade entre as bases teóricas em processo penal. Eric Sadin ainda alerta que o uso irrefletido da inteligência artificial pode conduzir à "emergência de um novo regime de verdade"[60]. No entanto, isso não parece suficientemente potente para a Comissão Europeia abrir mão do acesso pleno do quanto decidem os juízes e tribunais em processos penais. A publicidade aqui, fala mais alto e, mesmo que existam riscos nas pesquisas preditivas caso não se leve em conta que as máquinas são alimentadas por seres humanos e, nessa medida, os resultados das pesquisas podem advir de preconceitos, tendo isso como presente se aposta na possibilidade de construir sistemas peritos capazes de minimizar esses riscos. A ideia de dar preferência à publicidade das decisões e respectivo "accountability" acaba sendo defendida pelo embasamento conclusivo dos matemáticos Cristian Calude e Giuseppe Longo ao ponderarem que "nossos limitados ou "negativos" resultados, como ocorrem frequentemente (Longo 2008), não "destroem" a ciência de dados, mas abrem caminho para mais reflexões"[61], ou seja, no que concerne à Comissão Europeia, não é possível abandonar o quanto os algoritmos podem auxiliar na análise preditiva dos julgados e, assim, promoção de uma melhor prestação jurisdicional.

Quanto à possibilidade de as estatísticas gerarem compreensões equivocadas ou mesmo substituir a ciência, Cristian Calude e Giuseppe Longo ponderam que "na mesma medida que a análise de big data não pode substituir a ciência, nenhuma teoria pode ser tão boa para abandonar a necessidade de dados e testes"[62]. O ponto de equilíbrio, portanto, parece ser o melhor caminho encontrado pela Comissão Europeia nesses primeiros passos das pesquisas preditivas de jurisprudência no âmbito processual penal.

---

[60] SADIN, Eric. *Intelligence Artificielle ou l'enjeu du siècle (L')*: Anatomie d'un antihumanisme radical. Paris: L'Echappée, 2018, p. 81.

[61] CALUDE, Cristian; LONGO, Giuseppe. The Deluge of Spurious Correlations in Big Data. In: *Foundations of Science*. Vol. 22, Issue 3, pp. 595-612, DOI 10.1007/s10699-016-9489-4, 2017, p. 611..

[62] CALUDE, Cristian; LONGO, Giuseppe. The Deluge of Spurious Correlations in Big Data. In: *Foundations of Science*, Vol. 22, Issue 3, DOI 10.1007/s10699-016-9489-4, 2017, pp. 595-612, p. 611..

Considerações finais

Analisadas e compreendidas as questões técnicas que envolvem a adoção da inteligência artificial "fraca", é possível chegar a algumas conclusões a respeito dos questionamentos formulados na introdução e de como deve se dar o uso dessa ferramenta tecnológica na elaboração de pesquisas preditivas.

De partida é importante considerar os riscos de relacionamento entre o engenheiro do conhecimento e um perito em processo penal. Isso se dá não apenas pela difícil tradução de alguns temas de processo para uma linguagem algorítmica, mas pela ampla gama de diferentes visões de processo penal que hoje ainda coexistem e pela possibilidade de que as construções algorítmicas partam de entimemas. No mínimo, neste ponto, é preciso deixar claras as opções teóricas de processo penal para não confundir os intérpretes dos resultados que sejam produzidos nas pesquisas. Os vieses de análises, portanto, devem ser identificados, tornados claros e transparentes.

Tendo essas premissas em mente, as posturas antagônicas que vêm sendo adotadas pelos Estados Unidos e pela França, isoladamente vistas, não se apresentam como soluções adequadas. A criminalização de pesquisas preditivas promovida na França não é um caminho a ser seguido em termos de controles democráticos, pois aniquila a garantia da publicidade processual. Com efeito, a justificativa francesa pautada na privacidade dos julgadores colide com a publicidade processual e com a necessidade de prestação de contas à sociedade. E esta garantia processual penal deve prevalecer num aparente conflito, pois numa democracia quem exercita o poder tem o dever de prestar contas de seus atos. A publicidade das decisões judiciais diminui a possibilidade de abusos no exercício do poder e, como tal, é uma garantia processual fundamental que se sobrepõe ao interesse de privacidade dos julgadores.

Por outro lado, a preocupação do filósofo Eric Sadin no sentido de que o uso desenfreado da inteligência artificial possa conduzir à dependência dela na tomada de decisões, promovendo uma "emergência de um novo regime de verdade", não pode ser desconsiderada. E as pesquisas norte-americanas não parecem atentar para esses aspectos. A Comissão Europeia para a Eficácia da Justiça equilibra essa preocupação com a

invocação das ponderações dos matemáticos Cristian Calude e Giuseppe Longo de que "nenhuma teoria pode ser tão boa para abandonar a necessidade de dados e testes". A forma de neutralizar possível construção de novas verdades absolutas, passa pelo quanto anotado acima, isto é, tornar públicos e claros os vieses de construção dos algoritmos. Assim, esse meio termo sugerido pela Comissão Europeia, entre o radicalismo francês e a ausência de preocupação dos norte-americanos com a prevalência de "novos regimes de verdade", para seguir emprestando a preocupação de Eric Sadin, pode ser um caminho a ser também trilhado no Brasil, até porque, por aqui, já estão aparecendo pesquisas similares[63].

Portanto, evitar que os critérios de alimentação dos programas possam conduzir a resultados equivocados e estes, por sua vez, possam influenciar negativamente novas tomadas de decisão dos tribunais, ou, até mesmo, induzir a necessidade de reformas legislativas que diminuam direitos e garantias, deve nortear as pesquisas preditivas.

Muito ainda há para ser esclarecido, compreendido, empregado e delimitado no uso dessa nova tecnologia para fins preditivos, mas entre seguir um caminho de livre exploração, como parece indicar o percurso norte-americano, ou adotar uma solução radical inversa de criminalização da conduta, como está conduzindo a França nesse momento, a primeira opção, acrescida de uma dosagem maior de cautela nos moldes do quanto já documentado pela Comissão Europeia para a Eficácia da Justiça, parece ser o ponto de partida, devendo ser mantidas novas pretensões investigativas.

Referências

ADEODATO, João Maurício. Ética e Retórica: para uma teoria da dogmática jurídica, 5ª ed., São Paulo: Saraiva, 2012.

AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi. *Máquinas Preditivas*: a simples economia da inteligência artificial, tradução de Wendy Campos, Rio de Janeiro: Alta Books, 2018.

[63] LAGE-FREITAS, André; ALLENDE-CID, Héctor; SANTANA, Orivaldo; OLIVEIRA-LAGE, Lívia de. Predicting Brazilian court decisions. In: *arXiv.org*. Ithaca: Cornell University, 1905.10348v1 [cs.SI], 20 de abril de 2019.

ARISTÓTELES. *Metafisica*. 2ª ed., tradução de Edson Bini, São Paulo: EDIPRO, 2012.

ARISTÓTELES. Analíticos Posteriores. In: *Órganon*, 2ª ed., tradução de Edson Bini, São Paulo: Edipro, 2010.

ARISTÓTELES. *Retórica*, tradução de Edson Bini, São Paulo: Edipro, 2011.

BARROS, Flaviane de Magalhães. *(Re)forma do Processo Penal*: comentários críticos dos artigos modificados pelas leis n. 11.690/08 e 11.719/08. Belo Horizonte: Del Rey, 2009.

BOSTROM, Nick. *Superinteligência*: caminhos, perigos e estratégias para um mundo novo, tradução de Aurélio Antonio Monteiro, Clemente Genil Penna, Fabiana Geremias Monteiro, Patricia Ramos Geremias, Rio de Janeiro: Darkside Books, 2018.

CALUDE, Cristian; LONGO, Giuseppe. The Deluge of Spurious Correlations in Big Data. In: *Foundations of Science*, vol. 22, Issue 3, DOI 10.1007/s10699-016-9489-4, 2017, pp. 595-612, p. 611, disponível em https://www.di.ens.fr/users/longo/files/BigData-Calude-LongoAug21.pdf, acesso em 08 de setembro de 2019.

COUTINHO, Jacinto Nelson de Miranda. Dogmática Crítica e Limites Linguísticos da Lei. In: *Diálogos Constitucionais: direito, neoliberalismo e desenvolvimento em países periféricos*. COUTINHO, Jacinto Nelson de Miranda; LIMA, Martonio Mont'Alverne Barreto (Organizadores). Rio de Janeiro: Renovar, 2006, pp. 225-232.

COUTINHO, Jacinto Nelson de Miranda. Sistema Acusatório e Outras Questões Sobre a Reforma Global do CPP. In: COUTINHO, Jacinto Nelson de Miranda e CARVALHO, Luis Gustavo Grandinetti Castanho (Organizadores) *O Novo Processo Penal à Luz da Constituição. (Análise Crítica do Projeto de Lei n. 156/2009, do Senado Federal)*. Volume 2, Rio de Janeiro: Lumen Iuris, 2011.

DEBESSONET, Cary G.; CROSS, George R. . *An Artificial Intelligence Application in the Law: CCLIPS, a Computer Program That Processes Legal Information*. In: *High Technology Law Journal*, Vol. 1, Issue 2, Fall, 1987.

DENNETT, Daniel C.. *Darwin's Dangerous Idea*: evolution and the meaning of life. New York: Simon & Schuster Paperbacks, 1995.

DESCARTES, René. O Discurso do Método. In: *Descartes: obras escolhidas*. Organizadores: J. Guinsburg, Roberto Romano e Newton Cunha. Tradução de J. Guinsburg, Bento Prado Jr., Newton Cunha e Gita K. Guinsburg. São Paulo: Perspectiva, 2010.

DOMINGOS, Pedro. *O Algoritmo Mestre*: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo, tradução de Aldir José Coelho Corrêa da Silva, São Paulo: Novatec, 2017.

DONGES, Niklas. A Complete Guide to the Random Forest Algorithm. In: *Built In*, 16 de junho de 2019. https://builtin.com/data-science/random-forest-algorithm, acesso em 02 de setembro de 2019.

EUROPA. Conselho da Europa. Comissão Europeia para a Eficácia da Justiça. *Carta Ética Europeia de Utilização da Inteligência Artificial nos Sistemas Judiciários e seu Entorno*, Estrasburgo: CEPEJ, 03 de dezembro de 2018. Disponível em https://rm.coe.int/charte-ethique-fr-pour-publication-4-decembre-2018/16808f699b, acesso em 09 de julho de 2019.

EUROPA. Conselho da Europa. Comissão Europeia para a Eficácia da Justiça, *Boîte à outils pour soutenir la mise en œuvre des Lignes Directrices sur la conduite du changement vers la cyberjustice*, Estrasburgo: CEPEJ,13-14 de junho de 2019, pp. 14-15, disponível em https://rm.coe.int/cepej-boite-a-outils-cyberjustice-fr-cepej-2019-7/168094ef3d, acesso em 09 de julho de 2019.

FERNANDES TEIXEIRA, João de. *Mentes e Máquinas*, Porto Alegre: Artes Médicas, 1998.

FERNÁNDEZ, Gregorio. Panoramas de los sistemas expertos, In: CUENA, José (org.) *Inteligencia Artificial*: sistemas expertos, Madrid: Alianza Editorial, 1986, pp. 23-52.

FRANÇA. Conseil Constitucionnel. *Décision nº 2019-778 DC du 21 mars 2019*, disponível em https://www.conseil-constitutionnel.fr/decision/2019/2019778DC.htm, acesso em 09 de julho de 2019.

GARCIA, Luiz Antônio Mendes. Perspectivas de Modernização da Justiça Brasileira, In: *Escola Superior do Ministério Público do Paraná*, 27 de junho de 2019, Curitiba: Ministério Público do Estado do Paraná. Disponível em: https://www.youtube.com/watch?v=JsAx7c0qwS4&feature=youtu.be. Acesso em 29 de junho de 2019.

GUIMARÃES, Rodrigo Régnier Chemim. *Atividade Probatória Complementar do Juiz como Ampliação da Efetividade do Contraditório e da Ampla Defesa no Novo Processo Penal Brasileiro*. (Doutorado em Direito de Estado). Tese, Universidade Federal do Paraná, Curitiba, 2017, disponível em https://acervodigital.ufpr.br/bitstream/handle/1884/41025/R%20-%20T%20-%20RODRIGO%20REGNIER%20CHEMIM%20GUIMARAES.pdf?sequence=2&isAllowed=y, acesso em 06 de julho de 2019.

GUIMERÀ, R., SALES-PARDO, M.. Justice blocks and predictability of us supreme court votes. In: *PloS One*, 2011; 6(11):e27188. pmid:22096533, disponível em https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0027188, acesso em 09 de julho de 2019.

HEIDEGGER, Martin. *Ser e Tempo*. 2ª ed., tradução de Márcia Sá Cavalcante Schuback, Petrópolis: Vozes, 2007.

KATZ, Daniel Martin; BOMMARITO, Michael J.; BLOCKMAN, Josh. A general approach for predicting the behavior of the Supreme Court of the United States, In: *PLoS ONE*, 12(4): e0174698. https://doi.org/10.1371/journal.pone.0174698, acesso em 09 de julho de 2019.

KAUFMAN, Dora. *A Inteligência Artificial irá Suplantar a Inteligência Humana?*, Barueri, SP: Estação das Letras e Cores, 2018.

KHALED JR., Salah H. *A busca da verdade no processo penal*: para além da ambição inquisitorial. São Paulo: Atlas, 2013.

LAGE-FREITAS, André; ALLENDE-CID, Héctor; SANTANA, Orivaldo; OLIVEIRA--LAGE, Lívia de. Predicting Brazilian court decisions. In: *arXiv.org*. Ithaca: Cornell University, 1905.10348v1 [cs.SI], 20 de abril de 2019. Disponível em https://arxiv.org/pdf/1905.10348.pdf, acesso em 07 de setembro de 2019.

LOPES JR., Aury. *Direito Processual Penal*. 10ª ed., São Paulo: Saraiva, 2013.

MARTIN, A. D.; QUINN, K.M.; RUGER, T.W.; KIM, P.T.. Competing approaches to predicting supreme court decision making, In: *Perspectives on Politics*, 2004; 2(4), pp. 761–767, disponível em https://www.cambridge.org/core/journals/perspectives-on-politics/article/competing-approaches-to-predicting-supreme-court-decision-making/12CB7F54E411F9EA07DFADBB82196B0B, acesso em 09 de julho de 2019.

MATHEWS, Eric. *Mente*: conceitos-chave em filosofia, tradução de Michele Tse, Porto Alegre: Artmed, 2007.

MCCARTHY, John; MINSKY, Marvin L.; ROCHESTER, Nathaniel; SHANNON, Claude. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, Agosto de 1955, disponível em http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf, acesso em 05 de julho de 2019.

MCCARTHY, John. Ascribing Mental Qualities to Machines, In: *Philosophical perspectives in artificial intelligence*, RINGL, M (ed.), Atlantic Highlands, N.J.: Humanities Press, 1979, Disponível em http://jmc.stanford.edu/articles/ascribing/ascribing.pdf, acesso em 05 de julho de 2019.

NIEVA FENOLL, Jordi. *Inteligencia artificial y proceso judicial*. Madrid: Marcial Pons, 2018.

NILSSON, Nils J. *The Quest for Artificial Intelligence*: a history of ideas and achievements. New York: Cambridge University Press, 2009.

PLETSCH, Natalie Ribeiro. *Formação da Prova no Jogo Processual Penal: o atuar dos sujeitos e a construção da sentença*. São Paulo: IBCCRIM, 2007, pp. 65 e ss..

PRIMO, Alex; COELHO, Luciano Roth. A chatterbot Cybelle: a experiência pioneira no Brasil, In: RAMOS, Roberto (org.) *Mídia, Textos e Contextos*. Porto Alegre: Edipucrs, 2001, pp. 259-276.

PRIMO, Alex; COELHO, Luciano Roth. Comunicação e inteligência artificial: interagindo com a robô de conversação Cybelle. In: MOREIRA DOS SANTOS, Gil. *O Direito Processual Penal*, Porto: Asa Edições, 2002.

MOTTA, L. G. M. et al. (Eds.). *Estratégias e culturas da comunicação*, Brasília: Editora Universidade de Brasília, 2002, pp. 83-106.

RUGER, T. W.; KIM, P. T.; MARTIN, A. D.; QUINN, K. M.. The supreme court forecasting project: Legal and political science approaches to predicting supreme court decisionmaking, In: *Columbia Law Review*, , New York: Columbia Law School, 2004; 104(4), pp. 1150–1209, disponível em https://www.jstor.org/stable/4099370?origin=crossref&seq=1#page_scan_tab_contents, aceso em 09 de julho de 2019.

RUSSELL, Stuart; NORVIG, Peter. *Inteligência Artificial*, 3ª ed., tradução de Regina Célia Simille, Rio de Janeiro: Campus Elsevier, 2013.

SADIN, Eric. *Intelligence Artificielle ou l'enjeu du siècle (L')*: Anatomie d'un antihumanisme radical. Paris: L'Echappée, 2018.

SEARLE, John R. *Intencionalidade*, tradução de Julio Fischer e Tomás R. Bueno. São Paulo: Martins Fontes, 2002.

SEARLE, John R. Minds, Brains and Programs, In: *The Behavioral and Brain Sciences*, 3, Cambridge University Press, 1980, pp. 417-457, disponível em https://www.law.upenn.edu/live/files/3413-searle-j-minds-brains-and-programs-1980pdf, acesso em 05 de julho de 2019.

SIMONS, G. L.. *Introdução à Inteligência Artificial*, tradução de Guilherme M. G. Dias Pires, Lisboa: Clássica Editora, 1986.

TASSE, Adel El; MILÉO, Eduardo Zanoncini; PIASECKI, Patrícia Regina. O Novo Sistema de Provas no Processo Penal. Comentários à Lei 11.690/08. Curitiba: Juruá, 2008.

TURING, Alan M.. Computing Machinery and Intelligence, In: *Mind, A Quarterly Review of Psychology and Philosophy, New Series*, vol. LIX, nº 236, Oxford University

Press, outubro de 1950, pp. 433-460, disponível em https://phil415.pbworks.com/f/TuringComputing.pdf, acesso em 05 de julho de 2019.

VILHENA, Roberto. O seu futuro depende do passado, In: *Casa do Saber*, 2019. Disponível em: https://www.youtube.com/watch?v=El5NgfCrDpk&feature=youtu.be, acesso em 01 de julho de 2019.

WARAT, Luis Alberto. *O Direito e sua Linguagem*, 2ª ed., Porto Alegre: Sérgio Antonio Fabris Editor, 1995.

WITTGENSTEIN, Ludwig. *Investigações Filosóficas*, 6ª ed., tradução de Marcos G. Nontagnoli, Petrópolis: Vozes, 2009.

Informações adicionais e declarações dos autores
(integridade científica)

Declaração de conflito de interesses (conflict of interest declaration): o autor confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

Declaração de ineditismo e originalidade (declaration of originality): o autor assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 10/07/2019
- Controle preliminar e verificação de plágio: 12/07/2019
- Avaliação 1: 12/07/2019
- Avaliação 2: 25/07/2019
- Avaliação 3: 01/08/2019
- Decisão editorial preliminar: 27/08/2019
- Retorno rodada de correções: 09/09/2019
- Decisão editorial final: 20/09/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editor-associada: 1 (CC)
- Revisores: 3

COMO CITAR ESTE ARTIGO:

GUIMARÃES, Rodrigo R. C. A Inteligência Artificial e a disputa por diferentes caminhos em sua utilização preditiva no processo penal. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1555-1588, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.260

Consequências e perspectivas da aplicação de inteligência artificial a casos penais

Consequences and prospects of the application of Artificial Intelligence to criminal cases

Gustavo Mascarenhas Lacerda Pedrina[1]

Universidade de São Paulo – São Paulo/SP

gumascarenhas@hotmail.com

http://lattes.cnpq.br/4122752912642517

https://orcid.org/0000-0003-1259-8428

Resumo: Este artigo tem como finalidade fazer uma análise da aplicação atual e das perspectivas do que se conhece popularmente por inteligência artificial ao direito penal. São analisadas duas vertentes do aprendizado da máquina (*machine learning*): a computação estatística e a análise preditiva. Discute-se as consequências e alternativas para o uso de técnicas de inteligência artificial diante dos avanços nas ciências do cérebro. Alguns pontos relevantes a respeito do tema são destacados para promover a discussão quanto a quais devem ser os próximos passos na área e quais as possíveis aplicações com o estado-da-arte da tecnologia atual.

Palavras-chave: Inteligência Artificial; Computação estatística; Análise preditiva; Cérebro.

Abstract: *This article aims to make an analysis of the current application and perspectives of what is popularly known by artificial intelligence to criminal law. Two aspects of machine learning are analyzed: statistical computation and predictive analysis. It discusses the consequences and alternatives for the use of artificial intelligence techniques taken the advances in the brain sciences, some relevant points on the topic are highlighted to*

[1] Doutorando, Mestre e Bacharel em Direito pela Universidade de São Paulo (USP). Research Fellow no Charles Houston Institute da Harvard Law School (EUA). Assessor de Ministro no Supremo Tribunal Federal.

promote discussions about future scenarios of this area and possible current applications.

Key-words: *Artificial Intelligence; Statistical computation; Predictive analysis; Brain.*

Introdução

O direito penal está em constante adaptação à sociedade, procurando aliar a ciência que produz com as correntes filosóficas de cada momento. A tendência atual, não só nessa área do conhecimento, mas no mundo como um todo, está no aumento do uso da tecnologia, notadamente o que se convencionou chamar de inteligência artificial (IA). As novas ferramentas podem, de fato, criar sistemas de justiça mais balanceados, com resultados mais justos em suas decisões, mas é preciso analisar os resultados dessas inovações técnicas sob o ponto de vista científico, com todas as cautelas e os testes que a ciência recomenda. Esse exame pode indicar melhores aplicações às novidades tecnológicas.

A inteligência artificial se apresentará, em breve, como a solução para certos problemas da humanidade, inclusive na confecção de cenários de estudo da mente humana. Embora seja improvável que esta última variável substitua totalmente o homem, é possível que ela ofereça cenários que simulem a tomada de decisão do ser humano e, ao fazê-lo, ajude-nos a entender as possíveis razões da ação.

Não se trata propriamente de desvendar o dilema do livre-arbítrio do ponto de vista médico, mas os avanços da tecnologia podem deixar no passado conceitos puramente eticizantes, baseados em crenças histórico-religiosas.

Para o processo penal, importa esclarecer que não há no seu uso a solução singular para o estabelecimento de procedimentos judiciais que levem à aferição da culpa de modo automático e equânime. Ainda

assim, é necessário esclarecer (1) se a máquina é capaz de substituir o julgador humano – ou se o será num futuro breve; (2) em que medida a tecnologia já existente pode ser utilizada e em quais seriam aplicações viáveis ao processo penal; (3) quais as perspectivas futuras de sua aplicação para a matéria.

É preciso tratar a tecnologia como uma técnica não-neutra e ainda em evolução, bem assim apresentar o real ponto de seu desenvolvimento, afastando mitos e versões não validadas de uso.

1. Cognição e inteligência artificial

A inteligência da máquina fascina há um bom tempo a humanidade. O conceito de Inteligência Artificial (AI na sigla em inglês) é atribuído ao cientista da computação John McCarthy, que cunhou o termo em 1955. Pode-se resumir o conceito como a projeção de uma rede computacional para executar um conjunto definido de ações e aprender com a experiência.[2] Alan Turing apresentou trabalhos seminais para a inteligência artificial ainda na década de 1950, que indicavam que a máquina poderia ser programada para aprender pelo mimetismo da inteligência humana.[3] No decorrer do século XX, o imaginário popular passou a traçar a mente, ainda sob influência da perspectiva dualista, como um computador do corpo – e se havia um "computador" no ser humano, o desafio seria reproduzi-lo artificialmente (há nisso uma herança da lógica defendida por Descartes, segundo a qual nenhum sistema puramente físico poderia pensar, raciocinar ou ser consciente).

Atualmente, assumimos que a disseminação da tecnologia, que leva à sensação de já haver a máquina atingido a inteligência própria, trouxe o paradigma da inteligência artificial quase perfeita. Embora comuns os programas de reconhecimento de rosto, de identificação de

---

[2] Stanford University. AI. Disponível em https://www-cs.stanford.edu/memoriam/professor-john-mccarthy Acesso em 18.07.2019

[3] "We may hope that machines will eventually compete with men in all purely intellectual fields. But which are the best ones to start with? Even this is a difficult decision." TURING, A. M., *Computing machinery and intelligence*. In: *Mind,* Oxford, Vol. LIX, Outubro de 1950. P. 460.

imagens, objetos e vozes, tradução simultânea e até de assessoramento financeiro, nem tudo é inteligência artificial. Há diversos mitos quanto a matéria. Pode-se ligar a televisão, o rádio ou acessar a internet, uma pessoa se depare com propaganda que reivindica que tal aplicação é inteligente, o que não é exatamente verdade. Para ser realmente inteligente a máquina deve aplicar noções de contexto, o que, apesar de possível, ainda é insólito e apresenta um nível de desenvolvimento muito aquém do que o propagandeado.

O que quase todas as aplicações existentes fazem é computação estatística – que de fato faz parte das teorias de aprendizado por máquinas (*machine learning*), mas não é exatamente *inteligente*: o computador apenas oferece de maneira autônoma a melhor resposta estatística para a questão colocada.

Em primeiro lugar, é importante notar que o ser humano – mais bem acabado exemplo de inteligência natural e objeto do desejo de mimetismo – não é uma criatura estatística. Trata-se de uma espécie com particularidades que a tornam única, sendo a principal delas a linguagem. Berwick e Chomsky sustentam que a linguagem é um sistema de organização de pensamentos e que apenas a espécie humana é capaz de fundir pensamentos em forma de linguagem gráfica.[4] Esse processo de fusão é estruturado, buscando sempre o caminho neural mais curto para uma resposta concatenada. O arranjo dessa rede complexa é a resposta do sistema cognitivo, fruto da evolução humana.

Em segundo, deve-se notar justamente a capacidade cognitiva do ser humano, que, com auxílio da linguagem gráfica, é capaz de construir cenários no passado, que fazem sentido no presente e ajudam a projetar o futuro. A linguagem nos possibilita essa construção de panoramas, levando-nos ao próximo ponto de destaque: a capacidade de contar e

[4] Os autores chamam o processo de "*Merge*" que aqui traduzimos, por aproximação, como "fusão", mas que é algo ainda mais complexo que propriamente uma fusão, tratando-se de característica inata ao ser humano, que o diferencia enquanto espécie: é uma operação que combina duas expressões para gerar uma nova expressão mais complexa, sem que se modifique ou descarte as duas expressões originais. Ver mais em BERWICK, Robert C., CHOMSKY, Noam, *Why only us: language and evolution*. Cambridge: MIT Press, 2017. P.102

entender histórias ("*storytelling*")[5]. Winston, diante dessas premissas, propõe a *Strong Story Hypothesis,* segundo a qual "os mecanismos que permitem aos humanos falarem, entenderem e recombinarem histórias separam a inteligência humana da de outros animais."[6]

A combinação da linguagem e dos contextos, a partir de cenários históricos, forma a cultura. A cultura, por sua vez, é elemento fundamental na caracterização das próprias emoções humanas: Barrett realizou experimentos que demonstram que as emoções humanas não podem ser tidas como padrões, elas variam de sociedade para sociedade e até de um indivíduo para outro[7].

Essas premissas são importantes para que se adquira uma visão básica quanto a matéria: entregar a resposta média não é fazer justiça. Um sistema de inteligência artificial que não possa contextualizar os aspectos subjetivos do sujeito em análise entregará necessariamente uma resposta injusta. No processo penal, conforme consigna Fenoll, isto pode ser ainda mais delicado:

> "No processo penal, a automação é mais complicada e perigosa. Um delito não é algo tão comum como um conflito civil e uma ameaça a condições pessoais – tanto do agressor quanto da vítima – que devem ser consideradas cuidadosamente."[8]

---

[5] Antes Winston propõe a *Inner Language Hypothesis*, segundo a qual "Human intelligence is enabled by a symbolic inner language faculty whose mechanisms support both story understanding and the querying of perceptual systems." WINSTON, Patrick. *The Strong Story Hypothesis and the Directed Perception Hypothesis*. AAAI Fall Symposium Series, 2011. Artigo digital. Disponível em https://dspace.mit.edu/bitstream/handle/1721.1/67693/Submitted.pdf?sequence=1&isAllowed=y Acesso em 09.07.2019. P. 6

[6] "The Strong Story Hypothesis: The mechanisms that enable humans to tell, understand, and recombine stories separate human intelligence from that of other primates" WINSTON, Patrick. *The Strong Story Hypothesis and the Directed Perception Hypothesis*. digital. Disponível em https://dspace.mit.edu/bitstream/handle/1721.1/67693/Submitted.pdf?sequence=1&isAllowed=y Acesso em 09.07.2019. P. 2

[7] Cf. BARRET, Lisa Feldman. *How emotions are made*: the secret life of the brain. Boston: Houghton Mifflin Harcourt, 2017.

[8] "*En el proceso penal, la automatización es más compleja y peligrosa. Al fin y al cabo, um delito no es algo tan frecuente como un conflicto civil y suele estar*

De fato, é preciso notar que não há nada propriamente estatístico na aquisição de elementos culturais ou na formação da cognição. O ser humano pode até ser afeito a padrões, mas a cognição deve ser diferenciada da racionalidade: nem todas as tomadas de decisão do cérebro humano são fruto da escolha racional, mas todas são certamente tomadas de acordo com princípios cognitivos[9], formados a partir de aspectos únicos do ser humano, muito distantes de serem mimetizados razoavelmente pela máquina. Por essa razão, não nos parece razoável a aplicação de qualquer programa que não seja capaz de *entender* as reações humanas para aplicações que de qualquer maneira impliquem no cerceamento da liberdade, ao menos no estado-da-arte atual da tecnologia. Ainda assim, como sugerimos no item 3, pode-se utilizar a tecnologia existente em situações isoladas no processo penal.

2. Aplicação atual: computação estatística

O aumento dos estudos e aplicações a respeito da inteligência artificial levanta questões éticas a respeito dos limites do uso da tecnologia. No direito, é notável o dado que mais de 30 estados norte-americanos utilizem atualmente programas de inteligência artificial para sugerir aos juízes sentenças e fianças. Todos estes programas utilizados hoje são baseados em computação estatística, mais precisamente em um esquema chamado de EBS (*evidence-based sentencing*).[10] Ocorre que apesar do nome, essas *evidências* são na realidade dados objetivos relacionados ao sujeito, como gênero e endereço.

---

lleno de circunstancias personales – tanto del reo como de la víctima – que deben ser consideradas cuidadosamente, incluso com más cuidado que el actual." Cf. FENOLL, Jordi Nieva, *Inteligencia artificial y processo penal.* Madrid: Marcial Pons, 2018. p. 36.

9 Isto tomando em conta um indivíduo responsivo e pleno de suas capacidades.

10 Cf. STARR, S., *Evidence-based sentencing and the scientific racionalization of discrimination*. Stanford Law Review, Setembro de 2013. Disponível em: https://ssrn.com/abstract=2318940 Acesso em 16.07.2019. p.2

Recentemente, o caso *Wisconsin* vs. *Loomis* levou a questão até a Suprema Corte estadunidense[11]. A defesa de Eric Loomis questionou o uso de um programa de inteligência artificial (o COMPAS – *Correction Offender Management Profiling for Alternative Sanctions* – produzido pela Equivant) por parte do Juízo para determinar a sua condenação a seis anos em regime fechado[12]. Loomis queria ter acesso aos critérios que levaram o robô algorítmico a recomendar sua pena – a Suprema Corte negou o recurso, assentando tratar-se de segredo industrial.

O COMPAS leva em consideração 137 itens, não necessariamente ligados a questões atinentes ao delito possivelmente praticado, como (i) se há antecedentes penais na família do réu ou (ii) se há ocorrências relacionadas a álcool e drogas envolvendo a pessoa em julgamento[13].

No estado da Virgínia, a utilização de algoritmos para estabelecer condenações já acontece há mais de dez anos. Caliskan-islam, Byron, e Narayaan já demonstraram o perigo no seu uso com tal fim[14]: algoritmos são necessariamente programados e essa programação pode conter um erro de viés ideológico[15]. Os pesquisadores demonstraram que sentenças produzidas por robôs algorítmicos, em relação a nomes geralmente atribuídos a pessoas de ascendência africana, são

---

[11] U.S. Supreme Court. Wisconsin vs. *Loomis*. Disponível em: https://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/16-6387.htm Acesso em 19.04.2019

[12] Disponível em https://harvardlawreview.org/2017/03/state-v-loomis/ Ver também http://www.nytimes.com/2005/01/02/magazine/sentencing-by--the-numbers.html, https://www.nytimes.com/2016/06/23/us/backlash-in--wisconsin-against-using-data-to-foretell-defendants-futures.html e https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software--programs-secret-algorithms.html Acesso em 19.04.2019.

[13] FENOLL, Jordi Nieva, *Inteligencia artificial y processo penal*. Madrid: Marcial Pons, 2018. p. 68

[14] Cf. CALISKAN-ISLAM, A. BRYSON, J.J, NARAYAAN, A. *Semantics derived automatically from language corpora necessarily contain human biases.* 2016. Princeton: Princeton University. Disponível em: http://randomwalker.info/publications/language-bias.pdf. Acesso em 19.04.2019.

[15] "Bias should be the expected result whenever even an unbiased algorithm is used to derive regularities from any data; bias is the regularities discovered." (Ibid., p. 01).

comumente mais duras do que aquelas que contêm nomes tradicionalmente europeus[16]-[17].

Ocorre que a aprendizagem de máquinas envolve um estágio de pré-processamento para melhorar a qualidade dos dados de entrada[18]. Esse pré-processamento, também chamado de rotulagem, pode ser automático ou humano. Há, portanto, uma primeira porta de entrada a resultados enviesados: se o dado for automatizado, as evoluções sociais serão absorvidas pelo algoritmo com atraso; se a programação for humana, ela dependerá das opiniões de seu programador. Além disso, se nesse processamento forem incluídos dados como raça, gênero e endereço, o algoritmo indicará, punições maiores para determinados grupos sociais já marginalizados.

Mas o maior problema é outro: por tratar-se de segredo industrial, é impossível saber com precisão como os itens levados em consideração são combinados (em que ordem e proporção, por exemplo) para sugerir sentenças ou fianças. Isso viola ao menos dois princípios caros ao direito

---

16 "We have shown that machine learning can acquire prejudicial biases from training data that reflect historical injustice. (...) We show for the first time that if AI is to exploit via our language the vast knowledge that culture has compiled, it will inevitably inherit human-like prejudices. In other words, if AI learns enough about the properties of language to be able to understand and produce it, it also acquires cultural associations that can be offensive, objectionable, or harmful. These are much broader concerns than intentional discrimination, and possibly harder to address. (...) Our results show that European-American names have more positive valence than African-American names in a state-of-the-art word embedding. That means a sentence containing a European-American name will have a higher sentiment score than a sentence with that name replaced by an African-American name. In other words, the tool will display a racial bias in its output based on actor and character names. We picked this example because the argument follows directly from our experiments on names. But our results suggest that other imprints of human racial prejudice, not confined to names, will also be picked up by machine-learning models." (Ibid., p. 10-11).

17 Cf. MONAHAN, J; SKEEM, J. Risk Assessment in Criminal Sentencing. *Virginia Public Law and Legal Theory Research Paper*, n. 53. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662082. Acesso em 19.04.2019.

18 Cf. KOTSIANTIS, S. B.; KANELLOPOULOS, D; PINTELAS, P. E. Data preprocessing for supervised learning. *International Journal of Computer Science*. Jornal digital. vol. 1, no. 2, 2006, p. 111-117.

penal e processual penal: o devido processo legal, já que é impossível contraditar dados sem que se saiba nem mesmo quais são, e a proporcionalidade, porque não se pode garantir que sejam realizadas sempre as mesmas operações.

O que esse tipo de programa faz não difere em nada daqueles de análise de risco geralmente empregados em operações financeiras, por exemplo. De acordo com dados atuariais, fornece-se uma sugestão de sentença para o Juízo que, em última análise, aplica superficialmente (i) a prevenção geral e (ii) busca inibir a reincidência[19]. Ambos os resultados, no longo prazo, tornam-se verdadeira profecia aos sujeitos-objeto da análise, já que não é comum que mudem, por exemplo, de gênero (e se o risco de homens adultos for maior para a reincidência em um determinado delito, o programa recomendará maior tempo de pena, por partir do pressuposto que o indivíduo precisa de mais tempo de *ressocialização* – este também um conceito discutível, aliás).

A aplicação ao processo penal da atual de inteligência artificial, baseada em computação estatística, concentra-se na sugestão de sentenças e nessa medida, entendemos, apresenta problemas instransponíveis, ao menos por hora, por violar princípios basilares à matéria.

3. Aplicações viáveis da tecnologia existente

Ainda que se ressalve a aplicação para o mais notável ato do processo, a sentença, é possível que se admita a utilização do que se chama de inteligência artificial para atos processuais diversos. Bons exemplos são (i) a aplicação de teses em tribunais a partir da leitura

[19] "The trend is called "evidence-based sentencing" (hereinafter EBS). "Evidence," in this formulation, refers not to the evidence in the particular case, but to empirical research on factors predicting criminal recidivism. EBS seeks to help judges advance the crime-prevention objectives of punishment by equipping them with the tools of criminologists—recidivism risk prediction instruments grounded in regression models of past offenders' outcomes. The instruments give considerable weight to criminal history, which is already central to modern sentencing schemes." Cf. STARR, S., *Evidence-based sentencing and the scientific racionalization of discrimination*. Stanford Law Review, Setembro de 2013. Disponível em: https://ssrn.com/abstract=2318940 Acesso em 16.07.2019. p.1

automática de processos, (ii) o estabelecimento de standards probatórios (iii) a busca por evidências nos autos e (iv) as formulações de perguntas pelas máquinas.

No primeiro caso, é importante perceber que a máquina, por tecnologia já existente, pode "ler" processos. Trata-se de OCR, do inglês *Optical Character Recognition* (Reconhecimento Ótico de Caracteres), um método aplicado de maneira a permitir que o conteúdo escrito em um documento no formato de imagem seja reconhecido e transformado em um arquivo de texto editável. Desde o final de 2018, o Supremo Tribunal Federal tem aplicado a técnica nos recursos extraordinários e agravos em recursos extraordinários que chegam a Corte. O robô-algorítmico apelidada de Victor interpreta os recursos e os separa por tema. Nos 27 temas mais recorrentes – que representaram aproximadamente 60%[20] dessas classes processuais em 2018 – o Victor é capaz de processar a devolução ao Tribunal de origem ante a aplicação de uma tese já aprovada pelo Supremo ou para sobrestá-lo até que decidida.

No segundo, é possível que, pela análise de casos análogos se defina a aplicação de *standards* probatórios. Um exemplo pode ser a quantidade de entorpecente que caracteriza a materialidade do crime de tráfico. A análise em bloco de processos com a aplicação de AI pode indicar a quantidade média que costuma indicar a traficância, auxiliando na definição de parâmetros ainda abstratos na jurisprudência.

No terceiro ponto, é possível treinar a máquina para isolar a evidências nos autos de modo a fornecê-las a investigação e a tomada de depoimentos, auxiliando nos testemunhos e diminuindo a presença de falsas memórias nas narrativas.

No quarto, pode-se instruir a máquina para fornecer perguntas ao Juízo de modo a estabelecer parâmetros mais neutros para as inquirições.

Em todas essas aplicações é necessário, contudo, que sejam públicos os critérios de estabelecimento dos algoritmos e os caminhos combinatórios estabelecidos pela IA, de modo a afastar qualquer possível viés.

---

[20] Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=388443 Acesso em 16.09.2019

4. O futuro: análise preditiva

Para Winston, a análise histórica é parte fundamental da formação cognitiva do ser humano. As histórias, segundo essa linha de pensamento, formariam, ao longo do amadurecimento do cérebro humano, os padrões sobre cada contexto social – a cultura do indivíduo (o que é também conhecido como "storytelling").

Na inteligência cognitiva, é preciso que o sujeito possa analisar cenários e tomar escolhas ainda que não racionais. Winston e seu grupo de pesquisa elaboraram uma aplicação capaz de, a partir de histórias comuns à cultura americana (de Shakespeare aos irmãos Grimm), aprender o que leva a determinadas ocorrências, como, por exemplo, o *regicídio*.[21] Partindo desses critérios, a máquina desenvolveu panoramas futuros e pode até mesmo identificar conceitos como *revanche* em histórias que não mencionavam a palavra. Isto prova que a análise preditiva consegue, se bem executada, identificar a intenção do agente, mesmo que esta não esteja explicitada.[22] A este processo de exame de cenários futuros de

---

[21] "With our Start Parser-enabled translator, we readily express the needed if–then rules in English. Flexibility illustrating examples follow, exactly as provided to Genesis. • If X kills Y, then Y becomes dead. • If X harmed Y and Y is Z's friend, then X harmed Z. • X wanted to become king because Y persuaded X to want to become king. • Henry may want to kill James because Henry is angry at James. • If James becomes dead, then James cannot become unhappy. As the examples show, rules can be expressed as if– then sentences or because sentences, with or without regular names, and possibly with the modifiers may or cannot. May marks rules that are used only if an explanation is sought and no other explanation is evident. Cannot marks rules that act as censors, shutting off inferences that would otherwise be made. In the example, we do not become unhappy when we are dead, even though killing involves harm and harm otherwise causes the harmed to become unhappy. Reflection-pattern descriptions are a bit more complicated. Here are two versions of revenge. • Revenge 1: X and Y are entities. X's harming Y leads to Y's harming X. • Revenge 2: X and Y are entities. X's harming Y leads to Y's wanting to harm X. Y's wanting to harm X leads to Y's harming X." WINSTON, Patrick. *The Strong Story Hypothesis and the Directed Perception Hypothesis*. AAAI Fall Symposium Series, 2011. Artigo digital. Disponível em https://dspace.mit.edu/bitstream/handle/1721.1/67693/Submitted.pdf?sequence=1&isAllowed=y Acesso em 09.07.2019. P. 4

[22] WINSTON, Patrick. *The Strong Story Hypothesis and the Directed Perception Hypothesis*. Disponível em https://dspace.mit.edu/bitstream/handle/1721.1/67693/Submitted.pdf?sequence=1&isAllowed=y Acesso em 09.07.2019. P. 8

acordo com critérios estabelecidos no passado e no presente damos o nome da análise preditiva.

A máquina já é capaz de realizar operações do tipo "*who-knows-what*", respondendo justificadamente perguntas sobre cenários de crimes e sobre as intenções dos sujeitos ao tomarem a ação, bem assim diferenciar os motivos de um crime. Veja-se o exemplo[23]:

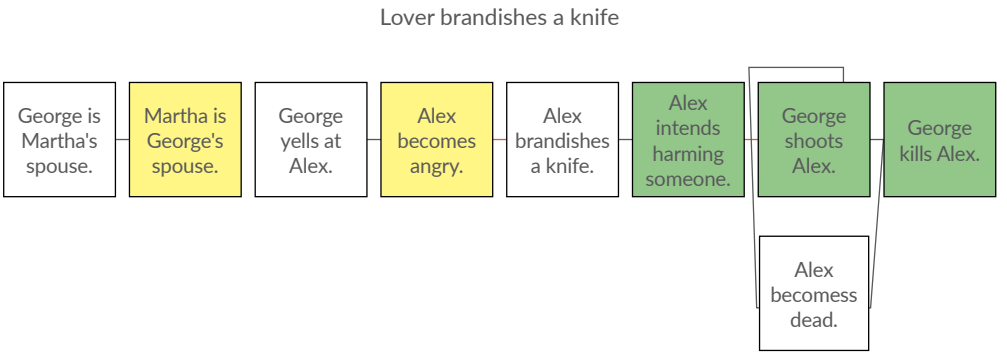


Figura 20: In the knife-brandishing version of a story raising a legal question, the elaboration graph indicates knife the brandishing is connected to the killing, suggesting *Self defense*.

[23] "Genesis can also compare two characters' perspectives, attributing differences in interpretation to differences in what is observed. The following records an exchange between a human questioner and the Genesis: Why does Jean Valjean disagree with Inspector Javert? Inspector Javert and Jean Valjean disagree about "Jean Valjean is criminal". Why does Jean Valjean think that Jean Valjean isn't criminal? Jean Valjean infers that Jean Valjean isn't criminal because [he] repents. Why did Inspector Javert think that Jean Valjean is criminal? Inspector Javert infers that Jean Valjean is criminal because [he] commits a crime. We believe that Genesis's who-knows-what ability sheds light on our human ability to reason about what others know and believe. Genesis's who-knows--what ability captures aspects of common sense (being within earshot, being unconscious or distracted, speaking over the phone or in another language), provides tools to aid in diplomacy and education (pinpointing differences in knowledge and experience), and suggests computational explanations of various psychological disorders (defects in mechanisms that enable understanding what others think)." WINSTON, Patrick, HOLMES, Dylan, *The Genesis enterprise: taking artificial intelligence to another level via computational account of human story understanding* Cambridge: MIT Computer Science and Artificial Intelligence Laboratory Center for Brains, Minds, and Machines, 2018. p. 28.

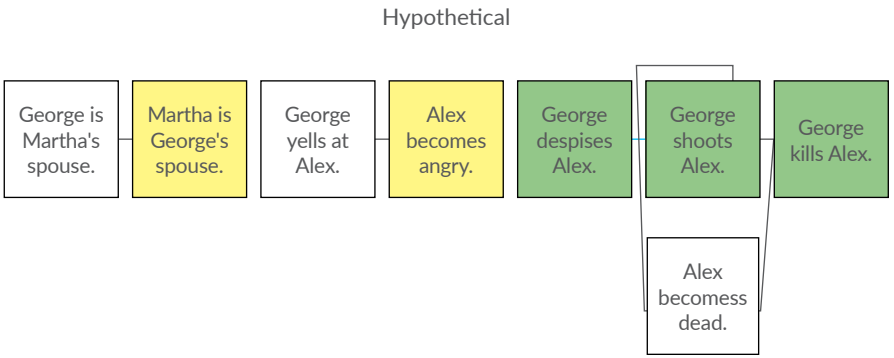


Figura 21: In the hypothetical version, with the brandishing removed, Genesis presumes the explanation for killing has to do with despising, suggesting guilt. At the concept level, *Self defense* becomes *Spiteful vengeance*.

Rabinowitz et al. Alcançaram resultados semelhantes com a aplicação ToMnet[24], também baseada em técnicas de análise preditiva. Vemos nisso um caminho aplicável da inteligência artificial ao direito penal e processual penal no futuro: ao invés de tê-la como um instrumento de medição atuarial de risco dos indivíduos, tem-se a possibilidade de com ela se aferir as intenções e qual era a real capacidade cognitiva de uma pessoa no momento de tomada de decisão ao cometer um crime.

Por se tratar de sistemas baseados em *storytelling*, os programas de inteligência lastreados na análise preditiva tomam em conta os aspectos subjetivos do sujeito, interpretando-os de acordo com o cenário apresentado. Este tipo de uso da tecnologia oferece cenários preditivos com elevado grau de certeza que dão conta dos *porquês* de um sujeito haver

[24] "We therefore extended the ToMnet to be able to make declarative statements about agents' beliefs. We achieved this by constructing a supervised dataset of belief states in the sample gridworld. We trained the UNREAL agents to report their beliefs about the locations of the four objects and the subgoal at every time step, alongside their policy. To do this, we added a head to the LSTM that output a posterior over each object's current location on the grid (or whether it was absent). During training, the agents learned to report their best estimate of each object's current location, based on its observations so far during the episode." RABOWITZ, N. C., PEBERT, F., SONG, H.F., ZHANG, C., ESLAMI, S.M.A., BOTVINIK, M., *Machine Theory of Mind*. Disponível em https://arxiv.org/abs/1802.07740 Acesso em 16.07.2019.

tomado certa decisão, podendo afetar, num futuro distante, até mesmo a culpabilidade – na medida em que pode entregar apreciação mais complexa da ação, vinculando a pessoa, de maneira individualizada, à conduta.

Esse tipo de utilização da tecnologia pressupõe, contudo, o aprendizado da máquina dos contextos em que cometido um delito e dos limites culturais envolvidos. Veja-se que não há ainda uma AI nesse nível de desenvolvimento, e que mesmo quando houver não será capaz de substituir o ser humano, cremos, na elaboração de sentenças ou atos que impliquem o cerceamento da liberdade do indivíduo. Poderá, ainda assim, fornecer ao julgador um cenário mais preciso do cometimento do crime, de modo a auxiliá-lo na tomada de decisão.

Pode-se reconhecer nesse tipo de aplicação uma melhor técnica para a instrução do processo-crime, a partir de parâmetros melhor delimitados, tornando mais rápido e preciso o processo penal.

Conclusão

Por se tratar de algo relativamente novo, ainda estamos aprendendo os reflexos das aplicações de inteligência artificial. Pode-se concluir do que estudado aqui que:

1. No ponto atual de desenvolvimento, a inteligência artificial não é comparável ao nível de desenvolvimento das redes neurais humanas, nem é capaz de substituir um julgador humano na determinação de atos que impliquem cerceamento da liberdade do indivíduo. A AI é desprovida de características básicas que fazem do julgador um ser humano, como emoções, capacidade de contextualização, cultura e linguagem.

2. Para se aliar, de forma válida, a inteligência artificial ao direito penal e processual penal os sujeitos não devem ser tratados de acordo com dados atuariais-objetivos. O uso de dados desse tipo em programas de inteligência artificial nos moldes em que ocorrem hoje nos EUA, para a sugestão de sentenças e fianças, podem aumentar a desigualdade social, levando ao encarceramento ainda mais concentrado de grupos já socialmente marginalizados.

3. É indispensável o estabelecimento de algoritmos claros e em acordo com preceitos constitucionais e de direitos humanos.

4. Há usos legítimos e ainda não explorados no processo penal para a AI no estado-da-arte atual, utilizando-a, por exemplo na (i) aplicação de teses em tribunais a partir da leitura automática de processos, (ii) estabelecimento de standards probatórios (iii) busca por evidências nos autos e (iv) formulações de perguntas pelas máquinas.

5. A técnica deve ser empregada sob o ponto de vista de garantia do indivíduo frente ao estado-juiz, nunca como elemento de prova pré-constituída de sua culpa. Trata-se, portanto, de meio de busca pela maior neutralidade possível no processo.

6. A análise preditiva é um caminho válido para o futuro da aplicação da inteligência artificial ao direito, estabelecendo cenários delituosos a partir de pontos de vista neutros que indiquem ao juízo um melhor nível de individualização da conduta. Para o processo penal especificamente, a utilização desse tipo de tecnologia pode resultar em maior precisão na instrução do processo-crime e melhores diretrizes decisórias ao julgador.

Referências

BARRET, Lisa Feldman. *How emotions are made*: the secret life of the brain. Boston: Houghton Mifflin Harcourt, 2017.

BERWICK, Robert C., CHOMSKY, Noam, *Why only us: language and evolution*. Cambridge: MIT Press, 2017.

CALISKAN-ISLAM, A. BRYSON, J.J, NARAYAAN, A. *Semantics derived automatically from language corpora necessarily contain human biases*. 2016. Princeton: Princeton University. Disponível em: http://randomwalker.info/publications/language-bias.pdf. Acesso em 19.04.2019.

FENOLL, Jordi Nieva, *Inteligencia artificial y processo penal*. Madrid: Marcial Pons, 2018.

KOTSIANTIS, S. B.; KANELLOPOULOS, D; PINTELAS, P. E. Data preprocessing for supervised learning. *International Journal of Computer Science*. Jornal digital. vol. 1, no. 2, 2006, p. 111-117.

MONAHAN, J; SKEEM, J. Risk Assessment in Criminal Sentencing. *Virginia Public Law and Legal Theory Research Paper*, n. 53. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662082. Acesso em 19.07.2019.

RABOWITZ, N. C., PEBERT, F., SONG, H.F., ZHANG, C., ESLAMI, S.M.A., BOTVINIK, M., *Machine Theory of Mind*. Artigo digital: Cornell University, 2018. Disponível em https://arxiv.org/abs/1802.07740 Acesso em 16.07.2019.

STARR, S., *Evidence-based sentencing and the scientific racionalization of discrimination*. Stanford Law Review, Setembro de 2013. Disponível em: https://ssrn.com/abstract=2318940 Acesso em 16.07.2019

TURING, A. M., *Computing machinery and intelligence*. In: *Mind,* Vol. LIX, Outubro de 1950.

WINSTON, Patrick. *The Strong Story Hypothesis and the Directed Perception Hypothesis*. AAAI Fall Symposium Series, 2011. Artigo digital. Disponível em https://dspace.mit.edu/bitstream/handle/1721.1/67693/Submitted.pdf?sequence=1&isAllowed=y Acesso em 09.07.2019.

WINSTON, Patrick, HOLMES, Dylan, *The Genesis enterprise: taking artificial intelligence to another level via computational account of human story understanding*. Cambridge: MIT Computer Science and Artificial Intelligence Laboratory Center for Brains, Minds, and Machines, 2018.

YUDKOWSKY, E. The Ethics of Artificial Intelligence. In: FRANKISH, Keith; RAMSEY, William. *The Cambridge Handbook of Artificial Intelligence*. New York: Cambridge University Press, 2014.

Informações adicionais e declarações dos autores (*integridade científica*)

Declaração de conflito de interesses (conflict of interest declaration): o autor confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

Declaração de ineditismo e originalidade (declaration of originality): o autor assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 22/07/2019
- Controle preliminar e verificação de plágio: 23/07/2019
- Avaliação 1: 30/07/2019
- Avaliação 2: 05/08/2019
- Decisão editorial preliminar: 23/08/2019
- Retorno rodada de correções: 18/09/2019
- Decisão editorial final: 24/09/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editora-associada: 1 (CC)
- Revisores: 2

COMO CITAR ESTE ARTIGO:

PEDRINA, Gustavo M. L. Consequências e perspectivas da aplicação de inteligência artificial a casos penais. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1589-1606, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.265

Fundamentos de Direito Processual Penal

Fundamentals of Criminal Procedure

O Processo Coletivo: primeiras impressões para a construção de uma nova dogmática processual

The Collective Process: first impressions for the construction of a new procedural dogmatics

Alexandre Rocha Almeida de Moraes[1]

Pontifícia Universidade Católica de São Paulo – São Paulo/SP

aram.mp@gmail.com

http://lattes.cnpq.br/9309967566132792

https://orcid.org/0000-0002-8374-5694

Rafael de Oliveira Costa [2]

Ministério Público do Estado de São Paulo – São Paulo/SP

rafaelcosta22000@gmail.com

http://lattes.cnpq.br/4793246077898855

https://orcid.org/0000-0001-9979-9382

Resumo: Como decorrência da coletivização dos litígios em âmbito penal e do descompasso com a tutela processual, exsurge uma nova área do conhecimento, denominada Direito Processual Penal Coletivo, instrumento do qual se vale o Estado para a imposição de sanção penal ao autor do fato delituoso que viola bens jurídico-penais coletivos, devendo primar pelo respeito aos direitos fundamentais e pela efetividade do

[1] Graduado, Mestre e Doutor pela Pontifícia Universidade Católica de São Paulo; Professor de Direito Penal da PUC/SP e da UNIFAAT; professor de diversas pós-graduações no país e Coordenador da Pós-Graduação em Direito Penal da Escola Superior do Ministério Público do Estado de São Paulo. Promotor de Justiça em São Paulo.

[2] Doutor e Mestre em Direito pela Faculdade de Direito da Universidade Federal de Minas Gerais; Graduado em Direito pela Faculdade de Direito da Universidade Federal de Minas Gerais, em programa conjunto com a Universidade de Wisconsin-Madison (Estados Unidos); Professor na Escola Superior do Ministério Público; Professor Visitante na Universidade da Califórnia-Berkeley; Promotor de Justiça no Estado de São Paulo.

sistema criminal. O presente artigo pretende problematizar questões que demandam a construção de um novo modelo de dogmática processual penal, seja inspirada no processo civil coletivo, seja sob a ótica dos litígios estruturais, além de discutir o papel do Ministério Público na atuação criminal coletiva.

Palavras-chave: processo penal coletivo; bens difusos e coletivos; ministério público.

Abstract: *As a result of the collectivization of litigations in the criminal sphere and of the lack of dialogue with the procedural protection, we are now facing a new branch of law, so-called Collective Criminal Procedure. It is an instrument used by the State to impose a criminal sanction on the perpetrator of the offense that violates collective rights, and is based on the respect of human rights and the effectiveness of the criminal system. The present article intends to problematize those that require the construction of a new model of procedural criminal dogmatics, whether inspired by the collective civil process or from the perspective of subsequent litigation, besides discussing the role of the Public Prosecution Service in its criminal activity.*

Keywords: *Collective criminal process; Different and collective goods; Public Ministry.*

1. INTRODUÇÃO

O tempo "é o árbitro supremo das épocas e das quadras históricas da sociedade humana" (DIP; MORAES, 2002, p. 252). A pós-modernidade e esse tempo social no contexto de um Estado Democrático e Social revelam que as últimas décadas foram marcantes para a transformação do papel do Estado e, em especial, do Ministério Público na proteção da sociedade.

Aliás, grande parte desse novo perfil do Ministério Público se deve ao modelo de Carta Constitucional que consagrou uma nova geração de direitos coletivos que passaram a ser, necessariamente, objeto de tutela.

É certo que qualquer tentativa de enquadrar a história em compartimentos estanques é altamente artificial, por uma única razão: as tradições clássicas do passado sobreviveram em certa medida, ainda que a sua influência contínua fosse um tanto precária e restrita.

De qualquer forma é fato que a revolução mercantil e o colonialismo (séculos XV e XVI), a revolução industrial e o neocolonialismo (séculos XVIII e XIX) e, atualmente, a revolução tecnológica, dos meios de comunicação e a globalização (séculos XX e XXI) formam três momentos diferentes do poder planetário. Os períodos de inquisição (século XV), os períodos derivados do iluminismo penal (séculos XVIII e XIX) e os períodos do positivismo *peligrosista* dão lugar, agora, a um período de incertezas no Direito Penal, ou ainda, para um campo aberto para a construção de novos paradigmas (MORAES; SMANIO, 2010).

Essa assertiva é válida para a dogmática penal, processual penal e para o próprio Ministério Púbico na área criminal. Na área penal, as novas demandas sociais decorrentes da aceleração do processo comunicativo e tecnológico passaram a exigir uma particular flexibilização na redação dos tipos penais já logo após a metade do século XX com os problemas e as novas formas jurídicas resultantes da chamada "economia de guerra" (ALFLEN DA SILVA, 2004 p. XXII).

Nesse diapasão, as leis penais em branco, 'cegas' ou 'abertas' (idealizadas por Binding), cuja exequibilidade depende do complemento de outras normas jurídicas ou da futura expedição de certos atos administrativos (regulamentos, portarias, editais) têm marcado a moderna dogmática penal (HUNGRIA, 1955, p. 96).

No direito processual penal, novos mecanismos de prova e de obtenção de prova (interceptação telefônica, colaboração premiada, infiltração de agentes, ação controlada etc.) convivem com os mecanismos tradicionais do modelo de inspiração iluminista.

E o Ministério Público brasileiro que ajudou a construir sua própria mudança constitucional, máxime na tutela dos bens difusos e coletivos, olvidou-se de se transformar ou demandar mudanças na tutela penal dos interesses transindividuais.

Como se sabe, o Direito, como produto da cultura humana para a tutela de interesses particulares (BARRETO 2001, p. 31), elevou-se à defesa e à conservação da sociedade. Além de interesses individuais e coletivos, passou a tutelar também interesses difusos e coletivos, apresentando ao processo penal um novo conceito de vítima: a sociedade.[3]

Mais recentemente, falam-se, inclusive, nos direitos fundamentais de quarta geração, cujo escopo abarcaria o direito à democracia, à informação e ao pluralismo, na tentativa de englobar todos os direitos fundamentais desenvolvidos anteriormente para a sedimentação de uma verdadeira globalização política, ao lado das globalizações econômica e cultural (CAVALCANTI, 2005, p. 115).

Diante desse panorama, é inegável assumir que houve contundente transformação subjetiva e objetiva na política criminal. Subjetivamente, novos gestores da moral, novas demandas e a incessante preocupação de

[3] "A summa divisio Direito Público e Direito Privado não foi recepcionada para fins de tutela jurídica e no âmbito do acesso à justiça pela Constituição da República Federativa do Brasil de 1988. A summa divisio constitucionalizada no País é Direito Coletivo e Direito Individual. Chega-se a essa conclusão porque o texto constitucional de 1988 rompeu com a summa divisio clássica ao dispor, no Capítulo I do Título II – Dos Direitos e Garantias Fundamentais, sobre os Direitos e Deveres Individuais e Coletivos. Dessa forma, considerando que no contexto do constitucionalismo democrático os direitos e garantias constitucionais fundamentais contêm valores que devem irradiar todo o sistema jurídico de forma a constituírem-se a sua essência e a base que vincula e orienta a atuação do legislador constitucional, do legislador infraconstitucional, do administrador, da função jurisdicional e até mesmo do particular, conclui-se que no contexto do sistema jurídico brasileiro a dicotomia Direito Público e Direito Privado não se sustenta." (ALMEIDA; COSTA, 2019, p. 71-72)

tutelar bens transindividuais (segurança viária, saúde pública, moralidade administrativa, criminalidade organizada e de massa, meio ambiente, patrimônio histórico, urbanismo, relações de consumo, ordem econômica etc.); já sob o aspecto objetivo, pode-se constatar a mudança de tempo e espaço (MORAES; SMANIO, 2010).

No direito penal contemporâneo, o Estado, para atender as demandas desse tempo-social tem recorrido, cada vez mais utiliza a criminalização de bens transindividuais e, nesse aspecto, o processo penal, deveria ser condizente com essa necessidade de demanda em termos de eficiência e garantias, sob a ótica do investigado e da sociedade (MORAES, 2016, p. 20).

Eis, pois, o grande dilema do Processo Penal contemporâneo: assentado no indispensável respeito aos direitos fundamentais e na eficiência do sistema criminal, ganha nova dimensão com a tutela dos bens jurídico-penais coletivos, que abrangem uma vasta gama de possibilidades: tutela dos investidores no mercado de valores mobiliários (Lei 7.913/89), do patrimônio público (Lei 8.429/92 e Lei 8.625/93), da ordem econômica e da livre concorrência (Lei 8.884/94), dentre outros.

Enfim, no recorte que interessa para o presente artigo, a Carta Política de 1988, seguindo tendência universal, reconheceu direitos e interesses de segunda (sociais) e terceira (difusos e coletivos) gerações, fornecendo – materialmente - instrumentos para garanti-los, dentre os quais e talvez o mais relevante: a nova feição e forma de intervenção do Ministério Público brasileiro.

Considerando que os bens jurídico-penais coletivos refletem efetivos direitos fundamentais e que possuem aplicabilidade imediata (art. 5º, §1º, da Constituição), o Estado deve disponibilizar toda a estrutura necessária à promoção de procedimentos penais coletivos, conferindo efetiva tutela a interesses tão caros a sociedade.

Nesse sentido, partindo-se de uma visão civilista da teoria geral do processo, Almeida e Mello Neto asseveram que se verifica que a Constituição impôs uma verdadeira mudança de paradigmas, sendo "necessária a construção de um conjunto de princípios, garantias e regras processuais adequados às necessidades do direito material coletivo como direitos fundamentais, conforme será observado no próximo tópico". (ALMEIDA; MELLO NETO, 2011, p. 82).

De outra parte, como espécie do gênero processo penal coletivo surgem em meados do século passado em julgamento pela Suprema Corte dos Estados Unidos os denominados "litígios estruturais"[4]. "Os denominados processos estruturais, diferentemente da matriz processual individual ou coletiva clássica que permeia o ambiente jurídico brasileiro, se apresentam de forma extremamente complexa, revelando um novo modelo de adjudicação de direitos, em contraposição ao modelo tradicional de resolução de disputas" (NUNES, COTA e FARIA, 2018, p. 365-367).[5]

Assim, ainda que como espécie de processo coletivo, o processo judicial de caráter estrutural seria aquele no qual "um juiz, enfrentando uma burocracia estatal no que tange aos valores de âmbito constitucional, incumbe-se de reestruturar a organização para eliminar a ameaça imposta a tais valores pelos arranjos institucionais existentes. Essa *injunction* é o meio pelo qual essas diretivas de reconstrução são transmitidas" (FISS, 2017, p. 120).

Partindo dessas premissas, o presente artigo pretende traçar os principais aspectos desse incipiente modelo que está se formando e, antes mesmo de traçar uma escolha metodológica sobre modelo a ser seguido, almeja problematizar as questões e institutos que tornam inevitável a construção um novo modelo de processo penal que busque um ponto de equilíbrio no que se deseja chamar de "Direito Processual Penal Coletivo", evitando os extremos do hipergarantismo e do punitivismo exacerbado.

---

[4] Suprema Corte Norte Americana, caso Brown *versus* Board of Education, de 17 de maio de 1954.

[5] "Talvez um dos mais importantes instrumentos nessa direção sejam as chamadas *structural injunctions*, concebidas pela doutrina norte-americana. Percebeu-se que muitas decisões sobre questões coletivas exigem soluções que vão além de decisões simples a respeito de relações lineares entre as partes. Exigem respostas difusas, com várias imposições ou medidas que se imponham gradativamente. São decisões que se orientam para uma perspectiva futura, tendo em conta a mais perfeita resolução da controvérsia como um todo, evitando que a decisão judicial se converta em problema maior do que o litígio que foi examinado" (ARENHART, Sérgio Cruz. Decisões estruturais no direito processual civil brasileiro. *Revista de Processo*, v. 225, 2013, p. 03).

1. NOVO TEMPO SOCIAL COMO CAUSA DE UMA NOVA DOGMÁTICA PENAL E PROCESSUAL PENAL

2.1. Características da sociedade moderna

O direito é produto cultural de um tempo-social e, justamente por isso, seria fácil precisar que o modelo de inspiração clássico-iluminista não existe mais em sua forma pura.

Com efeito, o modelo clássico (pena de prisão e garantias penais e processuais clássicas) já dera espaço ao Direito de *segunda velocidade* (política preponderantemente de barganha e de não persecução penal, inclusive aplicada aos bens difusos) e de *terceira velocidade* (em que se conjugam a flexibilização de garantias penais e processuais e a pena privativa de liberdade, com ênfase a uma política mais rigorista e de inimigos, como se dá na criminalidade organizada transnacional e no enfrentamento do terrorismo).[6]

Parte minoritária da doutrina, ademais, já aceita a ideia de uma quarta velocidade orientada pelo neopositivismo e pela possibilidade de aplicação de um Direito Penal internacional de um país soberano sob outro país igualmente soberano (PASTOR, 2006), assim como de uma quinta velocidade em que, em termos prospectivos, a dogmática não mais se preocupe com bens e interesses individuais, mas tão somente com bens transindividuais (STRATENWERTH, 2007).

O direito penal pós-moderno, não à toa, está carregado de um simbolismo que implica, simultaneamente, o excesso de criminalização estigmatizante e a proteção jurídica deficiente. Nessa esteira, segundo Hassemer, está se formando uma nova estrutura de Direito Penal material: caos normativo, descodificação da legislação, penas simbólicas e desproporcionais, tornando tábula rasa a ideia de fragmentaridade do direito penal (HASSEMER, 1993, p. 97).

Somente no Brasil, foram formatados mais 800 (oitocentos) novos tipos penais nos últimos trinta anos, com evidente aumento na moldura penal, criminalização territorialmente extensa e adoção de bens jurídicos

[6] Nesse sentido: Moraes, 2008, p. 33-34.

espiritualizados (supraindividuais, difusos, coletivos e individuais homogêneos) (MORAES, 2016, p. 21).

No entanto, o conjunto normativo penal editado pós-Constituição de 1988 possui pouco potencial de efetividade segundo o direito penal clássico (leia-se: aplicação da pena privativa de liberdade), pois basta ver que a transação penal é possível para cerca de 300 novos tipos; a substituição do art. 44 do CP, para mais de 600 novos tipos; o *sursis* processual para 420 tipos; e o *sursis*, para quase 630 tipos (MORAES, 2016, p. 15).

O aumento considerável das demandas penais, diante da tutela dos interesses difusos e coletivos e outros decorrentes da era pós-industrializada (crime organizado, terrorismo, delitos econômicos, de informática etc.), transformou o direito penal na principal forma de controle social.

É certo que a globalização econômica, a revolução dos meios de comunicação, a transnacionalização do crime, as novas formas de criminalidade econômico-financeira, os novos sujeitos passivos e os novos gestores da moral, aliados à evidente crise das tradicionais formas de controle social, contribuíram para esse retrato social e jurídico.

É certo, também, que o modelo de Estado Democrático Social e Constitucional, inexoravelmente, implicou movimentos de neocriminalização (FERNANDES, 2010, p. 22), máxime pelas características herdadas do modelo de bem-estar social e de uma sociedade de classes passivas (pensionistas, desempregados, destinatários de serviços públicos, consumidores etc.), que se convertem em 'cidadãos' e que passam a exigir do Poder Político a tutela dos seus novos interesses, até então, estranhos ao sistema jurídico de inspiração iluminista.

Mas é inevitável compreender que, ao lado da necessidade de proteção dessa nova geração de interesses e desses novos gestores da moral, um componente contribuiu, decisivamente, para a construção desse novo modelo de direito penal de bens transindividuais: a sociedade de riscos e a institucionalização de uma cultura prevencionista.

2.2. Sociedade de riscos e a sensação de insegurança

Os riscos sempre fizeram parte da existência humana em sociedade. Todavia, antes do advento da Revolução Industrial, os riscos eram

tidos e sentidos pela coletividade como oriundos de fatores externos e estranhos a ela.

Com a (r)evolução tecnológica, enquanto se minimizavam riscos externos, como doenças e catástrofes naturais, numa contradição apenas aparente, a sociedade humana passou a se expor a uma carga cada vez maior de riscos, inversamente proporcionais às facilidades decorrentes do desenvolvimento científico (LUHMANN, 1996, p. 17).

Se de início os riscos eram pessoais, durante a Idade Moderna Clássica os riscos assumiram uma nova dimensão, passando a atingir não mais indivíduos, mas antes coletividades; agora, na sociedade pós-moderna em que vivemos, os riscos passaram a atingir potencialmente toda a sociedade humana (MORAES, 2016, p. 35-37).

Nesse esteio, as novas demandas e os avanços tecnológicos repercutiram diretamente no bem-estar individual: a sociedade tecnológica, cada vez mais competitiva, passou a deslocar para a marginalidade um grande número de indivíduos, que imediatamente são percebidos pelos demais como fonte de riscos pessoais e patrimoniais, consolidando-se, pois, o conceito de 'sociedade de riscos' (BECK, 2010).

Assim, o surgimento de um 'direito penal do risco' (*Riskostrafrecht*) (PRITTWITZ, 2004, p. 44) que, longe de aspirar conservar o seu caráter fragmentário, como *ultima ratio*, tem se convertido em *sola ratio*, mais precisamente um direito penal expansivo, era uma consequência natural.

Os riscos modernos, acentuados pelas inovações trazidas à humanidade (globalização da economia e da cultura, meio ambiente, drogas, o sistema monetário, movimentos migratórios, aceleração do processamento de dados etc.), invariavelmente geram uma reação por parte dos atingidos: disso decorre a insegurança e o medo que têm impulsionado frequentes discursos postulantes de uma tutela da segurança pública, em detrimento de interesses puramente individuais.

É evidente que a sensação de insegurança decorrente deste modelo de 'sociedade de riscos', certamente é acentuada pela atuação da mídia e dos meios de comunicação que, raramente, projetam um debate público de maneira serena, equilibrada e fechada às excitações e incitações.

Enquanto, anteriormente, germinaram instrumentos de proteção da intimidade e da vida privada, o novo sistema penal do Estado, replicante do vigilantismo eletrônico, é extremamente invasivo e cultua a delação (ALFLEN DA SILVA, 2004, p. 93-94).

Em suma, os avanços tecnológicos e comunicação instantânea ensejaram uma nova vivência dos riscos e acentuaram a sensação subjetiva de insegurança o que, aliado ao discurso criminológico de baixo custo deu azo a uma considerável expansão legislativa (caos normativo de forma incongruente e desarrazoada); espacialmente, a globalização econômica, sem a consequente "Carta política mundial", desencadeou a perda da referência de valores e das fronteiras, tornando o crime também globalizado (MORAES; SMANIO, 2010).

Segurança pública, meio ambiente, ordem urbanística, sistema financeiro, ordem tributária, segurança viária, relações de consumo dentre outros, passaram a serem temas que atingem as pessoas de forma indistinta, tornando todos, sem percepção clara de tempo e espaço, em vítimas difusas.

Se for certo que pode haver certo exagero na extensa criminalização sem racionalidade e sem a construção de uma dogmática apropriada, também é possível reconhecer que o Ministério Público, como colegitimado na tutela de interesses difusos e coletivos, necessita se afeiçoar - como verdadeiro protagonista - para uma tutela eficiente, racional e equilibrada desses novos bens, não reiterando os excessos, nem tampouco protegendo de forma deficiente essa nova geração de direitos. Além disso, vários desses novos interesses transindividuais ingressaram no ordenamento jurídico sob a forma de microssistemas (Código de Trânsito, Crimes Ambientais, Lei Maria da Penha, Estatuto da Criança e do Adolescente etc), demandando a formação de profissionais menos especialistas e com visão transversal, multidisciplinar e mais resolutivos.

Seria, nesse contexto, possível a construção de uma nova dogmática processual em âmbito penal que concilie os ideais da promoção da Justiça e da eficiência? Para enfrentar esse dilema e na eventual busca de um novo modelo, será preciso compreender como a construção histórica dos direitos de segunda e terceira gerações se confundem com a recente feição institucional do Ministério Público brasileiro dada pela Constituição de 1988.

3. TUTELA PENAL DOS INTERESSES DIFUSOS

3.1. Breve Escorço Histórico da Tutela Coletiva

Não existe consenso na doutrina acerca da origem histórica da tutela coletiva (NEVES, 2016, p. 33-35). Em países que adotam o sistema do *civil law*, parcela dos estudiosos sustenta que a tutela coletiva teve seu nascedouro com as *actiones populares* do Direito Romano (ALMEIDA, 2003, p. 41). Os países que adotam o sistema do *common law*, por sua vez, sustentam que a tutela coletiva teve origem com a prolação de decisões pelas cortes inglesas que atingiam uma coletividade de jurisdicionados (*compulsory joinder rule*), nas quais ocorria a formação de situação similar a de um "litisconsórcio multitudinário" (LEAL, 1998, p. 25).

No Brasil, a ação popular é tida como a primeira manifestação da tutela coletiva. O instituto possibilitava a defesa de bens da coletividade pelo cidadão e foi prevista inicialmente pelas "Ordenações do Reino", encontrando posterior amparo no artigo 157, da Constituição de 1824 (MANCUSO, 2002, p. 52-54). Já a Lei n° 7.347/1985, chamada de Lei da Ação Civil Pública, inovou em inúmeros aspectos, especialmente na regulamentação da legitimidade ativa.[7]

Ademais, a Constituição de 1988 consagrou os direitos materiais coletivos como direitos fundamentais, ampliou as hipóteses de cabimento da ação popular (conforme o art. 5º, LXXIII, que passou a admiti-la para: (a) anulação de ato lesivo ao patrimônio público ou de entidade de que o estado participe; (b) anulação de ato lesivo à moralidade administrativa; (c) anulação de ato lesivo ao meio ambiente e ao patrimônio histórico e cultural), estabeleceu que o Ministério Público tem como função

---

[7] Ressalte-se que paira divergência na doutrina e na jurisprudência acerca da utilização das expressões "ação coletiva" e "ação civil pública": 1) uma primeira corrente entende tratar-se de sinônimas (BUENO, 2007, v. 1, p. 210); 2) outra parcela sustenta a distinção das expressões, dividindo-se em duas subcorrentes principais: a) a "ação civil pública" é modalidade proposta exclusivamente pelo Ministério Público, enquanto as "ações coletiva" podem ser ajuizadas por quaisquer outros legitimados (MAZZILLI, 2002, p. 73-74); b) a "ação civil pública" é a que tutela direitos difusos e coletivos e a "ação coletiva" é aquela utilizada para a defesa de direitos individuais homogêneos (ZAVASCKI, 2009, p. 56-58).

institucional a promoção do inquérito civil e da ação civil pública – para a proteção do patrimônio público e social, do meio ambiente e de outros interesses coletivos (artigo 129, inciso III) –, e previu em seu art. 5º, LXX, "a" e "b", o mandado de segurança coletivo.

Por fim, o Código de Defesa do Consumidor estendeu aos direitos individuais homogêneos a tutela conferida através do processo coletivo. Tudo isso sem prejuízo da legislação especial que trouxe, ainda que de forma pontual, importantes contribuições na evolução do processo coletivo.

Certo é, de qualquer forma, que essa legislação encontrou respaldo nos novos modelos de cartas constitucionais, aquilo que Canotilho (2003) denominou de "cartas dirigentes".[8]

3.2. Cartas dirigentes e a proteção dos interesses transindividuais

A Constituição de 1988, símbolo das novas cartas dirigentes, com índole comunitarista e analítica, buscou conferir um matiz constitucional ao direito penal. Mais que isso, procurou demonstrar a necessidade de tutela e proteção de outros interesses que já vinham demonstrando serem demandas da sociedade contemporânea (MORAES; SMANIO, 2010).

Segundo Von Liszt "é a vida, e não o Direito, que produz o interesse; mas só a proteção jurídica converte o interesse em bem jurídico"; argumentando ainda que "a necessidade origina a proteção, e, variando os interesses, variam também os bens jurídicos quanto ao número e quanto ao gênero" (VON LISZT, t. I, p. 94).

O direito penal pátrio passa pela transição do modelo de delito de lesão de bens individuais para o delito de perigo de bens supraindividuais: meio ambiente, patrimônio histórico e cultural, sistema urbanístico, sistema econômico e financeiro, ordem tributária, sistema previdenciário, saúde pública, incolumidade pública, bioética e biossegurança, educação, relações de consumo, probidade administrativa e segurança do trânsito são exemplos dessas novas demandas e interesses (MORAES; SMANIO, 2010).

Ocorre que diante desse fenômeno de constitucionalização do ordenamento jurídico, houve evidente transformação da sistemática da

[8] Ainda nesse sentido: Marques Neto (2005, p.72).

teoria do bem jurídico penal. A Constituição, legitimamente, é o indicador primário do bem que enseja tutela, máxime porque é, presumidamente, em termos de política criminal, onde o intérprete se socorrerá para aferir quais bens ou interesses representam maior "danosidade social" (MORAES; SMANIO, 2010).

Bricola, nesse diapasão, sustenta a "legitimidade da sanção penal somente diante da presença de uma violação a um bem que, ainda que não tenha o grau de relevância da liberdade pessoal que é sacrificada, está ao menos dotada de significação constitucional." (BRICOLA, 1973, p. 14, tradução livre).

O respeito à dignidade da pessoa humana (art. 1º), a redução das desigualdades sociais (art. 3º) e a realização de justiça social são, evidentemente, questões prioritárias ao Estado brasileiro e, pois, combater aquilo que ofende tais valores e bens implica em combater o que mais lesa a sociedade, ou seja, implica reconhecer a prioridade de proteção de bens jurídicos que digam respeito a tais valores (MORAES; SMANIO, 2010).

E, como se verá, para "zonas de danosidade social inequívoca" (BELLO, 2007, p. 264), há legitimidade material para a intervenção do Poder Público e deve, por excelência, o Ministério Público ocupar esse espaço em nome da sociedade.

3.3. A nova geração de bens jurídicos

Os bens jurídicos supraindividuais ou metaindividuais, como o próprio nome indica, transcendem ao individual. A expressão "bens espiritualizados", "interesses metaindividuais" ou "supraindividuais" inclui das categorias de interesses públicos e interesses coletivos em sentido amplo, enquanto estes se subdividem em individuais homogêneos, interesses coletivos estrito senso e interesses difusos.

Os direitos individuais homogêneos são aqueles de natureza divisível e de titularidade plúrima, decorrentes de origem comum. Já os direitos coletivos são aqueles comuns a uma coletividade de pessoas e apenas a elas e que repousam sobre "vínculo jurídico definido que as congrega" (como a sociedade comercial, o condomínio, a associação de pais etc.) (GRINOVER, 1984, p. 30).

Os bens difusos, por sua vez, são aqueles titularizados por uma cadeia abstrata de pessoas, configurando "interesses indivisíveis de grupos menos determinados de pessoas, entre as quais inexiste vínculo jurídico ou fático muito preciso' (MAZZILLI, 1996, p. 7). O vínculo fático une os titulares do direito difuso, "apesar de não existir uma vinculação jurídica que unifique os inumeráveis titulares, conglomerando-os em uma massa identificável de indivíduos; entre eles existe uma vinculação fática, consistente no simples fato de que todos o são do mesmo bem jurídico". (SMANIO, 2000, p. 108). Para Smanio:

> Os bens jurídicos penais difusos são aqueles concernentes à sociedade como um todo, dos quais os seus membros, individualmente considerados, não possuem disponibilidade, e que são indivisíveis e traduzem uma conflituosidade social (exemplos: a proteção do meio ambiente, a proteção das relações de consumo, a proteção da saúde pública, a proteção da economia popular, da infância e juventude, dos idosos etc). O que nos indica se os bens são tidos por bens jurídicos penais difusos ou não é o caso concreto, ou seja, através da análise da conduta praticada [...]. Ao se buscar identificar quais bens jurídicos difusos possuem relevância (dignidade) penal e carecem de tutela penal, devemos utilizar como filtro os princípios acima abordados, tendo sempre em vista as peculiaridades do caráter difuso do bem jurídico. (SMANIO, 2000, p. 108-109).

O conceito de bem jurídico na esfera penal vem ganhando importância, uma vez que sua principal função é a de legitimar e dar validade às normas penais; daí decorre o princípio da exclusiva proteção do bem jurídico onde não pode haver norma sem proteção ao bem jurídico.

A Constituição não estabelece explicitamente todos os bens jurídicos penalmente tutelados, concedendo ao legislador ordinário certa liberdade na escolha, desde que não vá de encontro com os princípios garantidores dos direitos fundamentais, principalmente limitando o poder de punir do Estado.

Smanio ressalta que as limitações que a Constituição de 1988 estabeleceu ao legislador penal estão previstas no artigo 5º, como direitos e garantias individuais e coletivos, citando como exemplos:

> 1º) Princípio da legalidade estabelecido no inc. XXXIX, da seguinte forma: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".
>
> 2º) Princípio da irretroatividade da lei penal estabelecido no inc. XL: "a lei penal não retroagirá, salvo para beneficiar o réu".
>
> 3º) Princípio da responsabilidade pessoal disposto no inc. XLV: "nenhuma pena passará da pessoa do condenado, podendo a obrigação de reparar o dano e a decretação de perdimento de bens ser, nos termos da lei, estendidas aos sucessores e contra eles executadas, até o limite do valor do patrimônio transferido".
>
> 4º) Princípio da presunção da inocência disposto no inc. LVII: "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória".
>
> 5º) Princípio da individualização da pena, determinado no inc. XLVI: "a lei regulará a individualização da pena e adotará, entre outras, as seguintes: a) privação ou restrição de liberdade; b) perda de bens; c) multa; d) prestação social alternativa; e) suspensão. (SMANIO, 2000, p. 47).

A seleção por parte do legislador do bem ou interesse difuso que demanda especial proteção máxime pelos efeitos de sua lesão ou ameaça de lesão deveria ser feita por parcimônia, máxime porque, como se verá, calcados na ideia de precaução e prevencionismo, alteraram profundamente a dogmática penal com a técnica de excessiva antecipação da tutela penal ou criminalização em estágio prévio.

3.4. Os bens difusos e o princípio da precaução

O aumento da criminalidade, com o passar dos anos, criou um ambiente favorável a uma política criminal mais rígida, com o intuito de reduzir riscos de agressões a bens jurídicos e de transmissão de segurança à sociedade.

A antecipação da tutela penal, ou aquilo que a doutrina alemã denomina de "criminalização em estágio prévio" (*Vorfeldkriminalisierung*)[9]

[9] V. nesse sentido: Bottini (2010, p. 50-51).

se dá basicamente pela utilização de crimes de perigo abstrato, pela criminalização autônoma de atos preparatórios, bem como pela crescente responsabilização da omissão imprópria.

Tenta-se, com isso, fazer com que o direito penal atue preventivamente com o fito de evitar danos futuros: a lesão ao bem difuso atinge o tecido social de forma difusa, gerando consequências mais sintomáticas e lesivas do que a simples violação de bens individuais ou individualizáveis.

Esse é, portanto, o paradoxo da política penal contemporânea: as novas demandas sociais e difusas e a dificuldade de se criminalizar direitos transindividuais, ou seja, a preocupação com danosidade social e fragmentariedade do direito penal em confronto com a necessidade de cautela na seleção dos bens jurídicos que mereçam tutela específica do direito penal e a forma pela qual os órgãos do sistema de justiça e segurança vêm atuando frente a esse novo modelo dogmático.

Se for certo que, dentre as instituições responsáveis pela repressão e prevenção da criminalidade, o Ministério Público teve que se aprimorar, paulatinamente, para uma proteção integral e efetiva de bens transindividuais, máxime através dos inquéritos civis, termos de ajustamento de conduta, ações coletivas etc, é certo que não se preparou para um atuar difuso e coletivo na proteção desses novos interesses em matéria criminal ou, ao menos, vem fazendo isso de forma casuística, isolada e sem uma sistematização que implique em reconhecer a necessidade de uma investigação criminal, de uma persecução e, enfim, de um processo penal coletivo.

4. UM NOVO RAMO DO DIREITO: O DIREITO PROCESSUAL PENAL COLETIVO

O paradigma coletivo acaba por promover uma nova percepção do direito penal e, consequentemente, do processo penal, especialmente em razão da insuficiência da tutela de bens jurídicos coletivos. E isso porque o Código de Processo Penal vigente faz incidir o direito penal de forma homogênea na tutela dos bens jurídicos individuais e coletivos, gerando situações anacrônicas, desproporcionais e injustas (ALMEIDA; COSTA, 2019).

É incongruente falar em um direito penal transindividual sem sustentar, por simetria, a ideia de um processo penal coletivo, dotado de um sistema de normas capaz de conferir respostas às demandas sociais (ALMEIDA, 2008).

Isso porque em grande parte das vezes, a solução para casos envolvendo bens transindividuais envolve a solução de litígios com alta carga de complexidade (*ex vi* os recentes casos de crimes ecológicos e crimes contra a vida nas barragens de Mariana e Brumadinho em Minas Gerais) e, pois, dilemas relevantes envolvendo a representação de interesses públicos e privados envolvidos e questões atinentes à legitimação extraordinária do Ministério Público, a própria resolução dos problemas e a efetiva proteção dos direitos envolvidos.

Nesse sentido, a proposta de (re)pensar o problema da tutela dos bens jurídico-penais coletivos se revela de grande utilidade para uma compreensão mais profunda do exercício da persecução penal, pois inaugura um novo enfoque, que prioriza o questionamento acerca do próprio fenômeno do direito processual penal. Isso porque a pretensão punitiva não pode ser exercida de forma discricionária e aleatória: ao contrário, a aplicação de uma sanção exige procedimento dotado de garantias e que assegure a adequada incidência da lei penal, inclusive no que concerne à tutela de bens jurídicos coletivos.[10]

No âmbito criminal, a Criminologia, a Política Criminal e o Direito Penal não são disciplinas estanques, mas complementares: representam três importantes aspectos, quais sejam, o explicativo-empírico (Criminologia), o decisional (Política Criminal) e o normativo (Direito Penal). A esses aspectos, acrescentamos ainda o viés executivo (Execução Penal) e o instrumental (Direito Processual Penal), agora dotado não apenas de um aspecto individual, mas também coletivo (Direito Processual Penal Coletivo).

Enquanto sistema único, comunica-se ainda com outras disciplinas (Medicina Legal, Sociologia, Filosofia, entre outras), compondo um saber transdisciplinar.

Nesse contexto, o Direito Processual Penal Coletivo é caracterizado pelo seu caráter dogmático e ausência de codificação própria, sendo responsável por fazer atuar o direito penal coletivo (caráter instrumental).

---

[10] Para uma análise aprofundada do tema, conferir: ALMEIDA; COSTA, 2019.

Ocorre que, tradicionalmente, o Processo Coletivo é classificado em duas categorias: o Processo Coletivo Comum e o Processo Coletivo Especial. Cada uma das espécies apresenta características próprias que a distingue da outra. A título exemplificativo, o Direito Processual Coletivo comum adota o princípio da disponibilidade motivada da ação coletiva, ao passo que no processo coletivo especial prevalece o princípio da impossibilidade de desistência da ação.

Contudo, abrem-se agora os horizontes para uma terceira espécie e que tem sido usualmente esquecida pela doutrina: o Direito Processual Penal Coletivo. Trata-se de área do conhecimento que deve observância a um conjunto de princípios, garantias, regras e deveres constitucionais e infraconstitucionais, através do qual são realizadas investigações e a persecução penal das infrações penais que atingem bens penais de titularidade coletiva, inclusive no que concerne à execução penal.

> Assim, a nota distintiva do Processo Penal Coletivo são os bens jurídicos tutelados, dotados de natureza coletiva – difusos, coletivos em sentido estrito ou individuais homogêneos. Não por outro motivo é que se pode sustentar que o Direito Processual Penal Coletivo possui natureza de garantia constitucional fundamental social." (ALMEIDA; COSTA, 2019, p. 141)

Em verdade, o Direito Processual Penal Coletivo tem como fundamento:

> O devido processo legal em sua dimensão social, na natureza constitucional dos bens jurídico-penais coletivos como direitos fundamentais da sociedade e no dever constitucional de organização dos procedimentos e dos processos penais coletivos. Em suma, trata-se de um novo paradigma de atuação, composto por um conjunto de princípios, regras, garantias e deveres processuais e procedimentais que disciplinam as investigações nas infrações penais que atinjam bens penais de titularidade coletiva, assim como as garantias processuais instrumentais de tutela coletiva em geral na área penal, incluída a tutela jurídica coletiva na execução penal e na defesa da segurança pública." (ALMEIDA; COSTA, 2019, p. 142)

De forma didática, pode-se conceituar o Direito Processual Penal Coletivo, nos termos do seu objeto formal, como:

> [...] a área do Direito Processual Penal composta por um conjunto de princípios, garantias, regras e deveres processuais constitucionais e infraconstitucionais que disciplina a ação penal coletiva, a jurisdição penal coletiva, o processo penal coletivo, a defesa no processo penal coletivo e a coisa julgada penal coletiva. Integra, assim, o Sistema do Direito Processual Penal Coletivo, o conjunto de princípios, garantias, regras e deveres processuais e procedimentais que disciplina as investigações nas infrações penais que atinjam bens penais de titularidade coletiva, assim como as garantias processuais instrumentais de tutela coletiva em geral na área penal, incluída a tutela jurídica coletiva na execução penal e na segurança pública. (ALMEIDA; COSTA, 2019, p. 145-146)

Partindo dessas premissas, o Processo Coletivo pode ser classificado da seguinte forma: 1. Processo Coletivo Comum, que se subdivide em a) Processo Coletivo Comum Cível e b) Processo Coletivo Comum Penal; 2. Processo Coletivo Especial, que se subdivide em: a) Processo Coletivo Especial Cível e b) Processo Coletivo Especial Penal.

Assim, o processo coletivo comum cível é caracterizado pela existência de um caso concreto a ser solucionado, ou seja, por um efetivo conflito de interesses ou uma ameaça de violação a um direito difuso, coletivo em sentido estrito, individual homogêneo ou individual indisponível. Trata-se de ramo que admite basicamente cinco diferentes espécies de ação: 1) a ação popular; 2) a ação civil pública; 3) a ação de improbidade administrativa; 4) o mandado de segurança coletivo; e 5) o mandado de injunção coletivo.

De outro modo, o processo coletivo comum penal é caracterizado pela violação *in concreto* de bens jurídico-penais de natureza coletiva. Em outras palavras, não se tutela bens jurídico-penais individuais ou a norma de forma abstrata, mas apenas casos nos quais tenha havido a violação concreta de bens jurídico-penais coletivos, *v.g.*, o meio ambiente, o patrimônio público, entre outros. Admite-se, para tanto, a utilização de diversas espécies de ações, dentre as quais se podem mencionar: 1)

a ação penal coletiva;[11] 2) o mandado de segurança coletivo criminal; e 3) o *habeas corpus* coletivo.

No que concerne ao processo coletivo especial, caracteriza-se pela ausência de solução de um conflito de interesses decorrente da violação ou ameaça de lesão a um direito difuso, cingindo-se à análise da constitucionalidade de lei em tese. Em outras palavras, tutela-se a coerência e integridade constitucional do ordenamento jurídico (direito difuso), preservando-o de eventuais violações, sem resolver o problema social. Divide-se em processo coletivo especial cível, quando tutela a integridade do ordenamento jurídico na esfera cível, e processo coletivo especial penal, quando analisa a constitucionalidade de norma sob o aspecto criminal.

Certo é, como brevemente salientado, que não se busca aqui traçar as linhas dogmáticas de um modelo de processo penal coletivo que poderia ser pensado sob a ótica do processo civil tradicional ou até mesmo sob a perspectiva dos processos estruturais.

De qualquer sorte, inevitável compreender que o aumento considerável de demandas complexas envolvendo bens jurídicos difusos vem exigindo do Poder Judiciário medidas que vão além de um simples julgamento de procedência ou improcedência da ação penal. No acertado dizer de Nunes, Cota e Faria, o Judiciário cada vez mais está sendo instado a decidir implementando políticas públicas ou aquilo que denominam de "medidas estruturais":

> Em suma, as medidas estruturais são aquelas que envolvem conflitos multipolares, de elevada complexidade, cujo objetivo é promover valores públicos e os direitos fundamentais pela via jurisdicional, mediante transformação de uma instituição pública

[11] A ação penal coletiva *"[...]* afigura-se como uma das principais figuras do Direito Processual Penal Coletivo, apresentando como característica distintiva da ação penal individual a tutela de direitos transindividuais. Em verdade, trata-se de demanda proposta por legitimado autônomo (Ministério Público) em defesa de um direito ou interesse coletivo amplamente considerado. A ação penal coletiva assume especial relevância quando atentamos para os crimes que afetam uma coletividade de pessoas, tal como sói acontecer com certos crimes contra a ordem econômica (v.g., dumping, combinação de preços entre concorrentes, dentre outros), contra o meio ambiente, contra as relações de consumo (v.g., crime de publicidade enganosa), os crimes de colarinho branco em geral, entre outros." (ALMEIDA; COSTA, 2019, p. 204-205).

> ou privada. Há a necessidade de reorganização de toda uma instituição, com a alteração de seus processos internos, de sua estrutura burocrática e da mentalidade de seus agentes, para que ela passe a cumprir sua função de acordo com o valor ou direito afirmado na decisão. Assim, essa nova tipologia de conflitos acaba por influenciar na conformação de um novo papel ao Poder Judiciário, de caráter gerencial e de consolidação de valores públicos. Outrossim, os litígios estruturais demandam o estabelecimento de um processo comparticipativo e marcadamente policêntrico, que seja capaz de abarcar os diversos interesses existentes, com o intuito de estabelecer uma relação dialógica e contínua para a concretização de direitos fundamentais e quebrar a lógica processual individual bipolar que ainda domina a seara processual. (NUNES, COTA e FARIA, 2018, p. 369)

Não se pretende traçar, portanto, a forma como deve se dar a tutela de bens jurídico-penais individuais ou a tutela do próprio ordenamento, mas do exercício da pretensão punitiva estatal nas hipóteses em que tenha havido a violação concreta de bens jurídico-penais coletivos.

A esfera criminal é a forma tradicional de atuação dos Membros do Ministério Público, uma vez que a Instituição, muito antes da Constituição de 1988, já era responsável pelo ajuizamento da ação penal pública. Contudo, até recentemente sequer se fazia a diferenciação dos instrumentos utilizados para o exercício da persecução em relação à natureza dos bens jurídicos tutelados (individuais ou coletivos em sentido amplo). Diante da insuficiência desse modelo, torna-se necessário problematizar os institutos processuais que compõem e demandam um novo paradigma.

Em verdade, a mudança deve ocorrer não apenas no plano legislativo, mas também na mentalidade dos operadores do Direito e dos membros do Ministério Público de modo a encampar a indispensabilidade da tutela transindividual, priorizando a máxima efetividade dos direitos coletivos. Para tanto, a tutela processual dos direitos coletivos em âmbito criminal admite toda e qualquer espécie de demanda ou pleito judicial, incluindo não apenas aqueles previstos na Constituição, mas todo o instrumental disponibilizado pelo Código de Processo Penal, pelo Código de Processo Civil, pelo microssistema Processual Coletivo e pela legislação especial que regulamenta a matéria (ALMEIDA; COSTA, 2019).

Nesse diapasão, o Direito Processual Penal Coletivo é responsável pelo adequado tratamento das questões afetas ao exercício da pretensão punitiva no âmbito do Direito Penal Coletivo. Aborda o crime sob o aspecto normativo-adjetivo, sempre com fulcro na tutela dos bens jurídico-penais coletivos, tal como sói acontecer com os efeitos da coisa julgada material coletiva, a colaboração premiada coletiva, a competência, dentre outros institutos.[12]

Diante desse cenário, o processo hermenêutico no Processo Penal Coletivo não pode ser aquele usualmente utilizado pelas demais disciplinas. Ao regulamentar o exercício da pretensão punitiva estatal em âmbito coletivo, é necessário atentar, resguardar e promover a dignidade humana e os sujeitos de direito atingidos pela infração penal em âmbito coletivo, o que torna extremamente complexa a sua concretização. Assim, a simplificação exegética é insuficiente para a solução de feitos penais coletivos, visto que a complexidade da temática, atrelada a necessidade de se conferir um tratamento interdisciplinar, exige a integração dos aspectos jurídicos, sociais, políticos, históricos e econômicos.[13]

Apenas a título exemplificativo, merece especial atenção merece o julgamento do *Habeas Corpus* Coletivo n° 143.641/SP, pelo Supremo Tribunal Federal. Trata-se de pedido formulado em favor de mulheres presas preventivamente que ostentam a condição de gestantes, de puérperas ou de mães de crianças sob sua responsabilidade, bem como em nome das próprias crianças, em virtude da nova redação conferida ao artigo 318, incisos III, IV e V, do Código de Processo Penal, pela Lei n° 13.257/16. Vejamos:

> Art. 318. Poderá o juiz substituir a prisão preventiva pela domiciliar quando o agente for: III - imprescindível aos cuidados especiais de pessoa menor de 6 (seis) anos de idade ou com deficiência; IV - gestante; V - mulher com filho de até 12 (doze) anos de idade incompletos.

---

12 Cf. ALMEIDA; COSTA, 2019.

13 Cf. ALMEIDA; COSTA, 2019.

O feito apresentou efetiva natureza coletiva, visto que a decisão abrangeu todas as pessoas "relacionadas no processo pelo DEPEN e outras autoridades estaduais, enquanto perdurar tal condição."

Ao final, a 2ª Turma do Supremo Tribunal Federal concedeu a ordem para determinar a substituição da prisão preventiva pela domiciliar - sem prejuízo da aplicação concomitante das medidas alternativas previstas no art. 319, do CPP - de todas as mulheres presas, gestantes, puérperas ou mães de crianças e deficientes, nos termos do art. 2º do Estatuto da Criança e do Adolescente e da Convenção sobre Direitos das Pessoas com Deficiências (Decreto Legislativo 186/2008 e Lei 13.146/2015), relacionadas no processo pelo DEPEN e outras autoridades estaduais, enquanto perdurasse tal condição.

O julgado tutelou direito individual homogêneo, nos termos do art. 81, parágrafo único, III, do Código de Defesa do Consumidor, visto que houve a apresentação, pelo DEPEN e por outras autoridades estaduais, de listas contendo os nomes e os dados das mulheres presas preventivamente que estavam em gestação ou eram mães de crianças sob suas guardas. Contudo, o STF estendeu a ordem de ofício a todas as demais mulheres presas, gestantes, puérperas ou mães de crianças e de pessoas com deficiência, bem assim às adolescentes sujeitas a medidas socioeducativas em idêntica situação no território nacional.

Em suma, não obstante a existência de discussão doutrinária sobre a forma como utilizado o remédio heroico, o HC n° 143.641/SP representou verdadeiro marco na jurisprudência do STF, coroando o novo paradigma coletivo na tutela penal no Brasil.

Dois obstáculos, contudo, existem à implementação do Direito Processual Penal Coletivo. O primeiro deles é a ausência de sistematização legal, ou seja, de um diploma normativo que unifique o tratamento da matéria, o que dificulta a adequada aplicação desse ramo do conhecimento. O segundo é a necessidade de uma mudança de mentalidade dos operadores do Direito, de modo a vislumbrar as potencialidades e limitações dos institutos processuais em âmbito coletivo.

Com o intuito de evitar uma abordagem superficial, este trabalho promove um recorte epistemológico. A abordagem holística exigiria uma análise de alguns institutos estruturais do Direito Processual Penal Coletivo, oque envolve, necessariamente, por força da cláusula pétrea

contida no art. 129, inciso I da Carta Magna uma crítica ao papel do Ministério Público brasileiro.

5. ESTADO DEMOCRÁTICO DE DIREITO, DIREITO PROCESSUAL PENAL COLETIVO E NOVO MODELO DE MINISTÉRIO PÚBLICO

Na defesa do regime democrático não é necessária apenas a garantia da defesa de direitos e liberdades contra o Estado, mas se "exige também a defesa dos mesmos contra quaisquer poderes sociais de facto" (MACHADO, 2007, p. 59). Nessa linha, "poderá afirmar-se que a ideia de Estado de Direito se demite de sua função quando se abstém de recorrer aos meios preventivos e repressivos que se mostrarem indispensáveis à tutela da segurança, dos direitos e liberdades dos cidadãos" (MACHADO, 2007, p. 59).

A Revolução Francesa no século XVIII impôs a democracia, governo do povo, pelo povo e para o povo, como a forma mais adequada de governo, ainda que não houvesse outra opção legitimamente cabível.

Ocorre que uma aparente democracia ou uma 'democracia de fachada' pautada pelas injustiças sociais de uma sociedade competitiva, com bolsões de desemprego e marginalidade, aumenta ainda mais a exigência de uma Política legislativa e criminal que atenda a um mínimo de racionalidade (MORAES; SMANIO, 2010).

A ordem constitucional brasileira, apesar de seu aparente espírito igualitário, não é capaz, por si só, de reverter o contexto de iniquidade social nem sequer de criar as condições políticas para a inclusão de setores expressivos da população nos quadros da cidadania formalmente regulada (CAMPILONGO, 2000, p. 56).

Diante desse cenário, resta evidente que essa ilusória democracia passa por crise profunda de legitimidade, seja porque a fé na democracia brasileira está abalada, seja porque não há acordo pacífico sobre quem é o 'povo'. Como se conceber, pois, um Estado Democrático de Direito em circunstâncias tais? (CAMPILONGO, 2000, p. 62).

A sobrevivência do Estado Democrático de Direito impõe, necessariamente, a proteção da moralidade e da probidade administrativa

nos atos administrativos em geral, exaltando as regras de boa administração e extirpando da gerência dos negócios públicos agentes que ostentam inabilitação moral para o exercício de funções públicas (MARTINS JR., 2001, p. 2). Nesse diapasão, Campilongo realiza um perfeito diagnóstico da questão:

> Nossas instituições representativas caracterizam-se pela completa irresponsabilidade política. Fogem de todas formas de controle e prestação de contas. Sustentam um sistema de dominação privatizado, de troca de favores com o Executivo e de partidos oportunistas. Em última análise, a negação de todos os princípios republicanos. [...] Nas palavras de O'DONNELL, temos uma 'cidadania de baixa intensidade', onde os direitos políticos são respeitados às custas do não reconhecimento dos direitos liberais à maioria da população. (2000, p. 57-59).

5.1. A necessidade de uma política criminal mais efetiva

Como é cediço, proteger bens transindividuais implica adotar escolhas racionalmente difíceis, tanto no tocante à seleção desses bens, quanto no tocante à técnica para positivação que, como se demonstrará, tem sido utilizada na forma de antecipação da tutela: tipificação de atos preparatórios e adoção de tipos de perigo abstrato, normas penais em branco, tipos omissivos impróprios e infrações de mera conduta, entre outros (MORAES; SMANIO, 2010).

Ao tratar da ação penal para defesa de interesses difusos, Mazzilli sustenta que o direito de punir não configura interesse difuso, nem coletivo, nem individual homogêneo: como decorrência ou expressão direta da soberania estatal, seria interesse público em sentido estrito (MAZZILLI, 2004, p. 211).

Em que pese a argumentação do Ilustre jurista no sentido de que a defesa da probidade administrativa "não envolve interesse transindividual (de grupos, classes ou categorias de pessoas), mas sim interesse público primário (bem geral da coletividade)" (MAZZILLI, 2004, p. 173), parece-nos mais acertada a natureza de bem difuso, defendida pela maior parte da doutrina (MANCUSO, 1994, p. 86), eis que se verifica, nesta

hipótese, vítimas indeterminadas, além da falta de visibilidade imediata dos danos causados.

Firmadas tais premissas, reconhecida a transição do modelo de política criminal por conta dos novos bens e demandas da sociedade moderna, questiona-se: mudou o Ministério Público para a prevenção criminal e atuação criminal difusa na proteção de bens difusos e coletivos? A resposta parece ser, ao menos por ora, negativa.

No afã de se construir um direito penal consentâneo com o constitucionalismo e com os anseios sociais contemporâneos -, impende serem intensificados de forma robusta e transparente os laços de condicionamento entre Democracia e direito penal (MANCUSO, 1994, p. 86).

Além do art. 127, da Carta Política, faz-se necessário ressaltar o disposto no art. 37, da Constituição, que apresenta prescrição ao Ministério Público de caráter vinculativo: a pretensão político-normativo configura um dever-ser. Em outros termos, a administração pública direta e indireta de qualquer dos Poderes e de qualquer dos entes federativos obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência (MORAES; SMANIO, 2010).

Como se vê, o Direito já está previsto, assim como o instrumento[14]. Tudo legitimado materialmente, eis que previsto na Lei Maior. Falta, ao que parece, uma regulamentação jurídica através de um microssistema que forneça uma segurança jurídica maior para esse novo modelo de atuação, mas antes disso, como sempre foi a tradição do Ministério Público brasileiro: falta que seus membros assumam, com evidente mudança cultural, seu papel de protagonista na defesa desses interesses essenciais ao Estado Republicano, à Democracia e à sociedade (MORAES; SMANIO, 2010).

5.2. Proposta de uma nova intervenção do Ministério Público na construção de um Sistema de Direito Processual Penal Coletivo

Mudou a sociedade, mudou o Direito. E o Ministério Público precisou e vem precisando se aperfeiçoar a essas transformações.

[14] Art. 129, I e II c/c art. 127, CF.

Bello, nesse sentido, destaca que "instituições como o Ministério Público possuem enorme responsabilidade no exercício e na inspeção de missões republicanas de valorização da coisa pública como o combate à corrupção", eis que, como é sabido, o pensamento republicano é tradicionalmente concebido enquanto elemento embasador de teorias de formas de governo e da liberdade, norteadas pela ideia central de *res publica* (coisa pública ou comum a todos os cidadãos) (BELLO, 2007, p. 264-265).

Partindo dessas premissas, a nova intervenção do Ministério Público no Processo Penal Coletivo exige uma mudança cultural e, consequentemente, normativa.

Embora o tratamento dispensado à matéria pela doutrina seja incipiente, o membro do Ministério Público deve estar preparado para atuar em conformidade com os novos paradigmas. Para tanto, deve utilizar de forma eficiente e "estratégica" os instrumentos e métodos de investigação, bem como os recursos extrajudiciais e judiciais disponíveis, visando, ainda, à prevenção e à tempestiva correção dos danos causados pelos delitos que afetam bens jurídicos coletivos (BECK, 2010). E mais: é necessário atuar sob a perspectiva do "litígio estratégico".

Os litígios estratégicos, conhecidos no Direito Norte-americano como *public interest litigation* ou *high impact litigation*, buscam realizar transformações sociais a partir da consolidação de precedentes sobre temas emblemáticos, os quais acabam por influenciar a implementação de políticas públicas:[15]

> [...] o litígio estratégico busca por meio do uso do judiciário e de casos paradigmáticos, alcançar mudanças sociais. Os casos são escolhidos como ferramentas para transformação da jurisprudência

[15] "Quanto aos demais objetivos, mudanças legislativas e nas políticas públicas, é necessário que seja possível um diálogo entre a decisão judicial e o Poder Executivo, provocando-o a ter uma atenção especial em relação à temática na gestão de suas políticas públicas, e também com o Poder Legislativo, ordenando-o ou fomentando-o a editar/alterar leis que deem aplicabilidade e concreção aos direitos discutidos em juízo. Grande exemplo dessa situação ocorre no caso do mandado de injunção (artigo 5º, inciso LXXI da CF/88 e Lei nº 13.300 de 2016) em que se busca a defesa de direitos subjetivos em face da omissão do legislador" (VINCENZI; ALVES; REZENDE, 2016, p. 224).

> dos tribunais e formação de precedentes, para provocar mudanças legislativas ou de políticas públicas. (CARDOSO, 2011, p. 365-366)

As ações penais coletivas refletem bem o ideal de litigiosidade estratégica, uma vez que envolvem amplo espectro social (VINCENZI; ALVES; REZENDE, 2016, p. 226). Assim, o litígio estratégico, especialmente no âmbito do Processo Penal Coletivo, difere do andamento processual em âmbito individual. Trata-se de uma combinação de técnicas jurídicas, políticas e sociais que abrangem desde a fase pré-processual até a prolação da sentença, buscando alcançar efetivas mudanças na esfera social (COSTA, 2017, p. 13).

Como bem acentuam Almeida e Mello Neto,

> A principiologia que rege o Direito Coletivo (princípio democrático, solidariedade coletiva, transformação social, aplicabilidade imediata dos direitos coletivos fundamentais, etc.) deve traçar a nova forma de atuação do Estado brasileiro e das suas instituições de defesa social, impondo o surgimento no País de um constitucionalismo inovador e comprometido com a implantação de uma sociedade mais livre, justa e solidária, nos termos dos Objetivos Fundamentais da República Federativa do Brasil, consagrados expressamente no art. 3º da CF/88. (2011, p. 84-85)

Assim, o conceito de litígio estratégico a ser adotado pelo Membro do Ministério Público deve envolver não apenas "situações de usual negativa à ampliação no reconhecimento de um determinado direito a um grupo de pessoas combinadas a uma possível inércia do Poder Legislativo" (VINCENZI; ALVES; REZENDE, 2016, p. 223) em normatizar a matéria, utilizando-se "o Poder Judiciário por meio de casos com potencial paradigmático, no intuito de: a) possibilitar a formação ou mudança de precedente junto às Cortes Supremas (STF e STJ); b) fomentar a discussão a respeito de mudanças legislativas; e c) provocar alteração nas políticas públicas" (VINCENZI; ALVES; REZENDE, 2016, p. 223), mas também a uma atuação teleológica, voltada para a uniformidade na atuação ministerial (evitando que promotores adotem posições distintas em feitos coletivos similares), a celeridade na tramitação do feito, a "desburocratização" do andamento processual (v.g., evitando a interposição de recursos que podem implicar

na mudança de decisão secundária e de somenos importância) e a máxima efetividade na tutela dos interesses da sociedade. (COSTA, 2017, p. 14).

Adotados estes fundamentos, surge a questão acerca das formas de atuação do Ministério Público no Direito Processual Penal Coletivo. Tradicionalmente, as formas de atuação do Ministério Público no Processo Coletivo são divididas em duas categorias, quais sejam, parte e fiscal da ordem jurídica.

A distinção só tem razão de ser quando o termo "parte" faz referência às "partes na demanda". Nesse caso, o Ministério Público atua tanto como parte, como fiscal da ordem jurídica. De outro modo, quando se toma como base a ideia de "partes no processo", todas as formas de atuação ministerial estão incluídas no conceito de parte, seja como autor, réu ou fiscal da ordem jurídica (NEVES, 2016, p. 261-262).

No que concerne ao polo ativo, o Ministério Público tem ampla legitimidade para a propositura da ação penal coletiva, em conformidade com o artigo 129, inciso I, da Constituição. Isso porque a Carta Magna sustenta expressamente que incumbe ao Ministério Público promover, privativamente, a ação penal pública, na forma da lei, não fazendo qualquer distinção quanto à ação penal individual e a coletiva. Assim, inviável a realização de exegese restritiva.

Essa cláusula pétrea – monopólio da ação penal pública – não deve ter seu exercício pautado pela obrigatoriedade: é da essência do processo penal coletivo e da tutela de bens difusos e coletivos a possibilidade, à luz de uma proteção suficiente e eficiente dos interesses transindividuais, a possibilidade de acordo.

Além disso, o art. 80, do Código de Defesa do Consumidor, estabelece que no processo penal atinente aos crimes que envolvam relações de consumo, poderão intervir, como assistentes do Ministério Público, os legitimados indicados no art. 82, inciso III e IV, aos quais também é facultado propor ação penal subsidiária, se a denúncia não for oferecida no prazo legal. Assim, ao disciplinar as entidades que podem figurar como assistentes do Ministério Público ou proporem a ação penal subsidiária, o Código do Consumidor encampou a legitimidade da Instituição para a propositura da ação penal coletiva.

No que concerne à possibilidade de formação de litisconsórcio por membros de Ministérios Públicos distintos, inexiste qualquer problema,

tendo em vista que incide subsidiariamente no âmbito processual penal coletivo o art. 5º, § 5º, da Lei n. 7.347/85, em atenção ao microssistema processual coletivo.

Ademais, óbice algum existe à atuação de determinadas entidades na qualidade de assistentes de acusação. Nesse sentido, os artigos 80[16] e 82[17] do Código de Defesa do Consumidor dispõem expressamente que, no processo penal atinente aos crimes que envolvam relações de consumo, poderão intervir, como assistentes do Ministério Público, as entidades e órgãos da Administração Pública, direta ou indireta, ainda que sem personalidade jurídica, especificamente destinados à defesa dos interesses protegidos pelo Código, e as associações legalmente constituídas há pelo menos um ano e que incluam entre seus fins institucionais a defesa dos interesses e direitos protegidos pelo Código.[18]

Do mesmo modo, o art. 26, parágrafo único, da Lei n. 7.492/86, admite a assistência da Comissão de Valores Mobiliários - CVM quando o crime tiver sido praticado no âmbito de atividade sujeita à disciplina e à fiscalização dessa Autarquia, e do Banco Central do Brasil quando, fora daquela hipótese, houver sido cometido na órbita de atividade sujeita à sua disciplina e fiscalização[19].

---

[16] Art. 80. No processo penal atinente aos crimes previstos neste código, bem como a outros crimes e contravenções que envolvam relações de consumo, poderão intervir, como assistentes do Ministério Público, os legitimados indicados no art. 82, inciso III e IV, aos quais também é facultado propor ação penal subsidiária, se a denúncia não for oferecida no prazo legal.

[17] Art. 82. Para os fins do art. 81, parágrafo único, são legitimados concorrentemente: III - as entidades e órgãos da Administração Pública, direta ou indireta, ainda que sem personalidade jurídica, especificamente destinados à defesa dos interesses e direitos protegidos por este código; IV - as associações legalmente constituídas há pelo menos um ano e que incluam entre seus fins institucionais a defesa dos interesses e direitos protegidos por este código, dispensada a autorização assemblear.

[18] Para uma análise aprofundada da matéria, conferir: ALMEIDA; COSTA, 2019, p. 211.

[19] Art. 26, parágrafo único - Sem prejuízo do disposto no art. 268 do Código de Processo Penal, aprovado pelo Decreto-lei nº 3.689, de 3 de outubro de 1941, será admitida a assistência da Comissão de Valores Mobiliários - CVM, quando o crime tiver sido praticado no âmbito de atividade sujeita à disciplina e à fiscalização dessa Autarquia, e do Banco Central do Brasil quando, fora daquela hipótese, houver sido cometido na órbita de atividade sujeita à sua

Igualmente, no âmbito dos processos penais coletivos, o Ministério Público atua como fiscal da ordem jurídica quando são ajuizadas ações penais coletivas subsidiárias, verificando a instauração e o desenvolvimento do processo, assim como o cumprimento da lei e da Constituição. Nesses casos, incumbe à Instituição aditar a queixa, repudiá-la e oferecer denúncia substitutiva, intervir em todos os termos do processo, fornecer elementos de prova e interpor recursos, em exegese analógica ao estabelecido pelo artigo 29, do Código de Processo Penal.[20]

Perceba-se que, uma vez ajuizada ação penal coletiva subsidiária e havendo negligência do autor da demanda, o Ministério Público poderá retomar a ação como parte principal, promovendo o seu devido andamento, de forma similar ao disposto no artigo 29, do Código de Processo Penal.[21]

A policentria é um paradigma de inúmeros casos envolvendo a lesão de bens individuais e, como tal, havendo vários atores direta ou mediatamente envolvidos, deve o Ministério Público tornar efetiva e concreta a participação dos beneficiados e atingidos para tornar concretamente legítima sua atuação como substituto processual[22]. Um dos dilemas a ser enfrentado na construção de um processo penal coletivo será, portanto, franquear canais e instrumentos distintos de participação na solução da causa, muito além da própria assistência litisconsorcial, como a realização de consultas e audiências públicas obrigatórias quando se tratarem de causas com alto grau de complexidade.

Ao lado dessas questões voltadas à atuação sob a forma de litígios estratégicos e novas formas de atuação no polo ativo da demanda, é preciso repisar e reconhecer que a atuação em um processo penal coletivo tende a se dar de forma preponderantemente extrajudicial (focada na prevenção), na forma de acordos, barganhas e não persecução penal (termos de ajustamento de condutas em matéria criminal), orientados por causas (sem necessária vinculação às definições territoriais e jurisdicionais hoje

---

disciplina e fiscalização. Para uma análise aprofundada da matéria, conferir: ALMEIDA; COSTA, 2019, p. 212.

20 Sobre o tema, conferir: ALMEIDA; COSTA, 2019.

21 Sobre o tema, conferir: ALMEIDA; COSTA, 2019.

22 V. nesse sentido o art. 2º, parágrafo único do PL n. 8058/2014, da Câmara dos Deputados que institui processo especial para o controle e intervenção em políticas públicas pelo Poder Judiciário e dá outras providências.

existentes) e, em especial, com orientação, sobre as prioridades de atuação de forma *interdependente* por laboratórios de jurimetria[23] (MORAES; DEMERCIAN, 2017).

Nesse sentido, o modelo de Agência[24] já defendido em Congresso Criminal do Ministério Público de São Paulo (MORAES; DEMERCIAN, 2017) representaria uma forma adequada de agir no âmbito do Direito Processual Penal Coletivo, permitindo a discussão, a implementação e a criação do futuro Sistema de Direito Processual Penal Coletivo, como historicamente se deu nas conquistas e novas atribuições institucionais.

Como bem acentuam Nunes, Cota e Faria, há um específico rol de princípios que compõem a fundação dos processos estruturais e que devem pautar a construção dessa nova dogmática processual: "o princípio democrático; o contraditório; a máxima amplitude da tutela jurisdicional coletiva; a harmonização dos valores em jogo; respeito e proteção da dignidade da pessoa humana; a atipicidade dos meios executivos, entre outros" (2018, p. 373)[25].

---

[23] Define-se a jurimetria em matéria criminal como ramo da Criminologia que utiliza a metodologia estatística para investigar o funcionamento do conjunto de normas penais e extrapenais, que se prestam à proteção de bens e servem como instrumento de controle social (MORAES, 2016, p. 274). O uso da jurimetria como mecanismo automático para subsidiar a forma de atuação repressiva (eficiência no combate à criminalidade com possibilidade verificação e controle externo da atividade policial e investigação criminal subsidiária), permitirá, naturalmente, prognósticos e a identificação de causas de agir na promoção de inquéritos civis e ações civis públicas por conta da violação de direitos sociais não implementados e que contribuem para alimentar as disfunções sociais. (MORAES; DEMERCIAN, 2017, p. 25).

[24] O modelo de agência – com promotores e procuradores de justiça, com analistas jurídicos, técnicos (peritos), analistas de dados ou de jurimetria, com a eleição de uma atuação preventiva e repressiva simultaneamente (inclusive com a colegitimação para a ação civil pública, para o inquérito civil etc) e, finalmente, mitigando a ideia de atuação vinculada ao poder judiciário, ao território e priorizando uma atuação voltada para as causas que podem ultrapassar limites territoriais tradicionais de uma comarca – é fundamental rever e conciliar os princípios institucionais previstos no §1º doa art. 127 da Constituição da República, de modo que convivam de modo harmônico na feição democrática que se espera do Ministério Público. (MORAES; DEMERCIAN, 2017, p. 25).

[25] Nesse mesmo sentido, buscando inovar na flexibilização dos tradicionais institutos do processo civil, veja-se o teor do PL n. 5139/2009 da Câmara dos Deputados.

Ao lado de se pensar uma forma de atuação pautada pelo membro do Ministério Público do fato (que resolva as questões de natureza cível e criminal de forma mais eficiente e resolutiva), de maior participação e consulta dos titulares diretos ou mediatos envolvidos e de uma nova estrutura de atuação do próprio Ministério Público orientada também pela discricionariedade e pela busca de acordos mais vantajosos para o interesse público e social como o mencionado modelo de agência, é preciso reconhecer que a própria ideia de execução, tal qual se dá no âmbito cível, deve ser repensada.

Nesse aspecto, relevante a sugestão de Nunes, Cota e Faria, segundo os quais, as partes estariam, dependendo do caso em litígio, autorizadas a definirem meios atípicos de execução, aptos à satisfação de direitos, desde fixados com vistas ao respeito e proteção da dignidade da pessoa humana: "a ampla participação, o contraditório pleno e a comparticipação abrem espaço para que os atores processuais negociem não apenas sobre o procedimento, mas também sobre o próprio direito material tutelado, apontando, em conjunto, para as soluções cabíveis, aplicáveis e efetivas para a mudança institucional que se espera" (2018, p. 376).

Enfim, essas primeiras ideias e problematizações almejam fomentar um repensar do processo voltado para a promoção de medidas estruturais, que permitam, por meio do Direito Processual Penal Coletivo, não só a adequada compreensão das características do litígio – em toda a sua complexidade e conflituosidade –, mas também a oitiva dos diferentes grupos de interesses, bem como a elaboração, a implementação e a fiscalização de um plano de "correção" do funcionamento das diversas instituições, tudo visando garantir efetivos resultados sociais.[26]

---

[26] Nesse sentido, Vitorelli conceitua o processo estrutural como sendo "um processo coletivo no qual se pretende, pela atuação jurisdicional, a reorganização de uma estrutura burocrática, pública ou privada, que causa, fomenta ou viabiliza a ocorrência de uma violação pelo modo como funciona, originando um litígio estrutural. Essencialmente, o processo estrutural tem como desafios: 1) a apreensão das características do litígio, em toda a sua complexidade e conflituosidade, permitindo que os diferentes grupos de interesses sejam ouvidos; 2) a elaboração de um plano de alteração do funcionamento da instituição, cujo objetivo é fazer com que ela deixe de se comportar da maneira reputada indesejável; 3) a implementação desse plano, de modo compulsório ou negociado e, 4) a fiscalização dos resultados da implementação, de forma a garantir o resultado social pretendido no início do processo, que é a correção

CONCLUSÕES

1. As últimas décadas foram marcantes para a transformação do papel do Estado e, em especial, do Ministério Público na proteção da sociedade.

2. Inúmeras mudanças ainda estão porvir, especialmente nesse tempo social pós-moderno, de transição e de riscos incalculáveis, em que novas demandas ao direito penal e processual penal são constantemente apresentadas.

3. A dogmática penal pós-88 demonstra a tentativa de se adaptar a essas novas realidades, ocasionando a coletivização dos litígios também na esfera criminal.

4. Contudo, o descompasso com a tutela processual tem impulsionado a necessidade de construção de uma nova área de conhecimento, denominada Direito Processual Penal Coletivo, da qual se vale o Estado para a imposição de sanção penal ao autor do fato delituoso que viola bens jurídico-penais coletivos e que prima pelo respeito aos direitos fundamentais e pela efetividade do sistema criminal.

5. Para além da sistematização legal, seja seguindo uma concepção civilista, seja de litígios estratégicos ou estruturais, a mudança de mentalidade dos operadores do Direito é fundamental, de modo a permitir uma verdadeira ruptura paradigmática com a forma de se ver e conceber uma atuação preventiva, preponderantemente extrajudicial, com juízo de oportunidade e possibilidade de acordos, investigativa e repressiva até então atrelada ao aspecto individual e que, invariavelmente, demandará uma atuação focada em causas e desvinculada das limitações jurisdicionais e territoriais hoje existentes.

6. Não se pretende no presente artigo construir o modelo de Direito Processual Penal Coletivo, mas tão somente alertar para

da violação e a obtenção de condições que impeçam sua reiteração futura." (VITORELLI, 2019, p. 1583).

os riscos associados à ausência de exploração dessa nova área, sob pena de prevalecer a impunidade ou ineficiência, em decorrência da ausência de efetividade e eficácia das técnicas usuais de combate à criminalidade em hipóteses de violações a bens jurídicos transindividuais, além de evidenciar a necessidade de que o Ministério Público brasileiro – como titular exclusivo da ação penal pública e como principal colegitimado a agir na tutela de bens difusos e coletivos – repense e discuta um novo modo de agir consentâneo com esse novo modelo, atuando de forma estratégica e promovendo medidas estruturais.

REFERÊNCIAS

ALFLEN DA SILVA, Pablo Rodrigo. *Leis Penais em Branco e o Direito Penal do Risco: Aspectos Críticos e Fundamentais.* Rio de Janeiro: Lumen Juris, 2004.

ALMEIDA, Gregório Assagra de. *Direito Processual coletivo brasileiro.* São Paulo: Saraiva, 2003.

ALMEIDA; Gregório Assagra de. COSTA, Rafael de Oliveira. *Direito processual penal coletivo* - A Tutela Penal dos Bens Jurídicos Coletivos: Direitos ou Interesses Difusos, Coletivos e Individuais Homogêneos. Belo Horizonte: D'Plácido, 2019.

ALMEIDA, Gregório Assagra de. *Direito Material Coletivo: Separação da Summa Divisio Direito Público e Direito Privado por uma nova Summa Divisio Constitucionalizada.* Belo Horizonte: Del Rey, 2008.

ALMEIDA, Gregório Assagra de Almeida; MELLO NETO, Luiz Philippe Vieira de. Fundamentação constitucional do direito material coletivo e do direito processual coletivo: reflexões a partir da nova summa divisio adotada na CF/88 (TÍTULO II, CAPÍTULO I). *Revista TST*, Brasília, vol. 77, n. 3, jul/set 2011.

ARENHART, Sérgio Cruz. *Decisões estruturais no direito processual civil brasileiro*. Revista de Processo,v. 225, 2013.

BARRETO, Tobias. *Introdução ao Estudo do Direito: Política Brasileira.* São Paulo: Landy, 2001.

BECK, Ulrich. *Sociedade de Risco – Rumo a uma outra Modernidade.* São Paulo: Ed. 34, 2010.

BELLO, Enzo. *Perspectivas para o Direito Penal e para um Ministério Público Republicano*. 1. ed. São Paulo: Lúmen Júris, 2007.

BOTTINI, Pierpaolo Cruz. *Crimes de Perigo Abstrato*. 2. ed. São Paulo: Revista dos Tribunais, 2010.

BRICOLA, Franco. *Teoria Generale del reato. Estratto dal "Nuovissimo Digesto Italiano"*. Torino: Utet, 1973, t. 9.

BUENO, Cassio Scarpinella. *Curso sistematizado de Direito Processual Civil*. São Paulo: Saraiva, 2007, v. 1.

CAMPILONGO, Celso Fernandes. *O Direito na Sociedade Complexa*. São Paulo: Max Limonad, 2000.

CANOTILHO, José Joaquim Gomes. *Direito Constitucional e Teoria da Constituição*. 7. ed. Lisboa: Almedina, 2003.

CARDOSO, Evorah. *Ciclo de vida do litígio estratégico no sistema interamericano de direitos humanos: dificuldades e oportunidades para atores não estatais*. Revista Electrónica del Instituto de Investigaciones Ambrosio L. Gioja, Ano V, número especial, 2011.

CAVALCANTI, Eduardo Medeiros. *Crime e Sociedade Complexa*. Campinas: LZN, 2005.

COSTA, Rafael de Oliveira. *Do Futuro do Ministério Público: Efetividade de Políticas Públicas e Litígio Estratégico no Processo Coletivo*. In: BARBOSA, Renato Kim (Org.). O Futuro do Ministério Público. São Paulo: APMP, 2017.

DIP, Ricardo; MORAES Jr., Volney Corrêa Leite de. *Crime e Castigo – Reflexões Politicamente Incorretas*. Campinas: Millennium, 2002.

FERNANDES, Antonio Scarance. *Processo Penal Constitucional*. 6. ed. São Paulo: Revista dos Tribunais, 2010.

FISS, Owen. *As formas de Justiça*. In: WATANABE, Kazuo (et al) (org.). *O Processo Para Solução de Conflitos de Interesse Público*. Salvador: JusPODIVM, 2017.

HASSEMER, Winfried. *Três Temas de Direito Penal*. Publicações Fundação Escola Superior do Ministério Público, 1993.

HUNGRIA Hoffbauer, Nélson. *Comentários ao Código Penal*. 3ª ed. Rio de Janeiro: Forense, v. I, Tomo 1°, 1955.

KUHN, Thomas S. *A estrutura das revoluções científicas.* São Paulo: Perspectiva, 2000.

LEAL, Márcio Flávio Mafra. *Ações coletivas: história, teoria e prática.* Porto Alegre: Sérgio Antonio Fabris Editor, 1998.

LUHMANN, Niklas. *Sociologia del Rischio.* Milão: Burno Mondadori, 1996.

FELDENS, Luciano. *Tutela Penal de Interesses Difusos e Crimes do Colarinho Branco.* Porto Alegre: Livraria do Advogado, 2002.

MACHADO, João Baptista. *Introdução ao Direito e ao Discurso Legitimador*. 1ª ed., Coimbra: Almedina, 2007.

MANCUSO, Rodolfo de Camargo. *Ação civil pública.* 8. ed. São Paulo: RT, 2002.

MANCUSO, Rodolfo de Camargo. *Interesses Difusos – Conceito e legitimação para agir*, 3ª edição, RT, 1994.

MARQUES NETO, Agostinho Ramalho. *Canotilho e a Constituição Dirigente.* 2 ed. Rio de Janeiro: Renovar, 2005.

MARTINS Jr, WALLACE PAIVA. Probidade Administrativa, Saraiva, 1ª edição, 2001.

MAZZILLI, Hugo Nigro. *A defesa dos interesses difusos em juízo.* 15. ed. São Paulo: Saraiva, 2004.

MORAES, Alexandre Rocha Almeida de. *Direito Penal Racional: Propostas para a Construção de uma Teoria da Legislação e para uma Atuação Criminal Preventiva.* Curitiba: Juruá, 2016.

MORAES, Alexandre Rocha Almeida de. *Direito Penal do Inimigo: A Terceira Velocidade do Direito Penal.* Curitiba: Juruá, 2008.

MORAES, Alexandre Rocha Almeida de; DEMERCIAN, Pedro Henrique. *Um novo modelo de atuação criminal para o Ministério Público brasileiro: agências e laboratório de jurimetria*, Revista Jurídica da Escola Superior do Ministério Público de São Paulo, v. 11 n. 1 (2017). Disponível em: <http://www.esmp.sp.gov.br/revista_esmp/index.php/RJESMPSP/ article/view/338>. Acesso em: 10 jul. 2019.

MORAES, Alexandre Rocha Almeida de; SMANIO, Gianpaolo Poggio. *Tutela penal da moralidade e probidade administrativas.* Tese apresentada e aprovada por unanimidade no I Congresso do Patrimônio Público e Social do Ministério Público do Estado de São Paulo, 2010. Disponível em: <http://www.mp.sp.gov.br/ portal/page/portal/Congresso%20PatPublico/ Teses/Alexandre%20e%20

Smanio%20-20TUTELA_PENAL_DA_PROBIDADEADMINIS TRATIVAtese.doc>. Acesso em: 10 jul 2019.

NEVES, Daniel Amorim Assumpção. *Manual de processo coletivo*. 3. ed. Salvador: Ed. JusPodivm, 2016.

NUNES, Leonardo Silva; COTA, Samuel Paiva; FARIA, Ana Maria Damasceno de Carvalho. Dos litígios aos processos estruturais: pressupostos e fundamentos. In: Juliana Cordeiro de Faria Ester Camila Gomes Norato Rezende Edgard Audomar Marx Neto (organizadores). *Novas tendências, diálogos entre direito material e processo*. Belo Horizonte: Editora D'Plácido, 2018.

PASTOR, Daniel Roberto. *La deriva neopunitivista de organismos y activistas como causa del desprestigio actual de los derechos humanos*. Jura Gentium – Rivista di filosofia del diritto internazionale e dela politica globale, 2006. Disponível em: <http://www.juragentium.org/topics/latina/es/pastor.htm>. Acesso em: 18 nov 2018.

PRITTWITZ, Cornelius. *O Direito Penal entre Direito Penal do Risco e Direito Penal do Inimigo: tendências atuais em direito penal e política criminal*. São Paulo: Revista Brasileira de Ciências Criminais, v. 47, mar./abr. 2004.

SMANIO, Gianpaolo Poggio. *Tutela Penal dos Interesses Difusos*. São Paulo: Atlas, 2000.

STRATENWERTH, Gunter. *La criminalización em los delitos contra biens jurídicos colectivos*. In: HEFENDEHL, v. Hirsch e Wohlers (Orgs.). *La teoria del bien jurídico. Fundamento de legitimatión del derecho penal o juego de abalorios dogmático?* Madrid: Marcial Pons, 2007.

VINCENZI, Brunela Vieira de; ALVES, Gustavo Silva; REZENDE, Priscilla Correa Gonçalves de. *As ações coletivas como espécie de litígio estratégico: Um diálogo com a luta social por reconhecimento de Axel Honneth*. Revista Jurídica Direito & Paz, v. 34, 2016.

VITORELLI, Edilson (Org.). *Manual de Direitos Difusos*. 2. ed. Salvador: JusPodivm, 2019.

VON LISZT, Franz. *Tratado de Direito Penal Alemão*. Rio de Janeiro: F. Briguet & C.,1899, T. I.

ZAVASCKI, Teori Albino. *Processo coletivo – Tutela de direitos coletivos e tutela coletiva de direitos*. 4. ed. São Paulo: RT, 2009.

Informações adicionais e declarações dos autores (*integridade científica*)

Declaração de conflito de interesses (conflict of interest declaration): os autores confirmam que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

- *Alexandre Rocha Almeida de Moraes*: projeto e esboço inicial, coleta e análise de dados, levantamento bibliográfico, revisão bibliográfica, redação, revisão crítica com contribuições substanciais, aprovação da versão final.

- *Rafael de Oliveira Costa*: projeto e esboço inicial, coleta e análise de dados, levantamento bibliográfico, revisão bibliográfica, redação, revisão crítica com contribuições substanciais, aprovação da versão final.

Declaração de ineditismo e originalidade (declaration of originality): os autores asseguram que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atestam que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 27/01/2019
- Controle preliminar e verificação de plágio: 09/03/2019
- Avaliação 1: 21/03/2019
- Avaliação 2: 24/03/2019
- Avaliação 3: 11/04/2019
- Deslocamento para V5N3 e aviso autores: 23/05/2019
- Decisão editorial preliminar: 03/07/2019
- Retorno rodada de correções: 23/07/2019
- Decisão editorial final: 16/09/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editor-assistente: 1 (ADR)
- Revisores: 3

COMO CITAR ESTE ARTIGO:

MORAES, Alexandre R. A.; COSTA, Rafael de O. O Processo Coletivo: primeiras impressões para a construção de uma nova dogmática processual. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1609-1648, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.223.

Processo penal em perspectiva interdisciplinar

Criminal procedure in an interdisciplinary perspective

A dissonância cognitiva e seus reflexos na tomada da decisão judicial criminal

The cognitive dissonance and its effects in the criminal judicial decision-making

Flávio da Silva Andrade[1]

Universidade Federal de Minas Gerais – Belo Horizonte/MG

flavio.andrade.ro@gmail.com

lattes.cnpq.br/9592306654276563

orcid.org/0000-0001-9571-6551

Resumo: O ensaio analisa a teoria da dissonância cognitiva, concebida por Leon Festinger, que se assenta na premissa de que o indivíduo experimenta um estado de desconforto psíquico quando percebe que há discrepância ou incoerência entre suas cognições ou atitudes, de forma que passa agir, voluntária ou involuntariamente, buscando diminuir ou afastar a dissonância e recuperar a sensação de coerência. Busca-se demonstrar como a dissonância cognitiva pode afetar o processo de tomada de decisões judiciais na esfera do processo penal, quando, por exemplo, o magistrado decide num sentido em sede de cognição sumária, mas, depois, em cognição exauriente, percebe não haver elementos bastantes para corroborar a avaliação inicial. Constata-se que o anseio por um estado de coerência e o interesse de preservar a autoimagem tendem a atrair o viés de confirmação a partir da evitação ou desconsideração de elementos dissonantes e da adição de novos elementos consonantes. Conclui-se que é justificada, nesse contexto, a aspiração pela adoção da figura do juiz de garantias e da prevenção como causa de exclusão da competência. E enquanto tramitam projetos de lei tendentes a implementar tais inovações, os juízes precisam ter consciência do fenômeno em questão, de maneira

[1] Doutorando e Mestre em Direito pela Universidade Federal de Minas Gerais. Juiz Federal do TRF da 1ª Região, titular da 4ª Vara da Subseção Judiciária de Uberlândia/MG.

a se tentar reduzir as chances de que caiam nas armadilhas de sua mente. O estudo realizado é do tipo exploratório-compreensivo, de vertente jurídico-dogmática, com prioridade para a análise de conteúdo.

Palavras-chave: Direito Processual Penal; Psicologia social; Dissonância cognitiva; Tomada de decisões judiciais criminais; Reflexos.

Abstract: *This essay analyzes the theory of cognitive dissonance, proposed by Leon Festinger, which is based on the premise that the individual experiences a state of mental discomfort when he realizes that there is discrepancy or inconsistency between his cognitions or attitudes, and he, voluntarily or involuntarily, changes his actions seeking to diminish or dispel dissonance and regain a sense of coherence. It is sought to demonstrate how cognitive dissonance can affect the process of judicial decision-making in the sphere of criminal proceedings, when, for example, the magistrate in summary cognition decides one way, but then, in exhaustive cognition, he realizes that there are not enough elements to corroborate his initial assessment. It is found that the desire for a state of coherence and the interest in preserving self-image tend to attract confirmation bias by avoiding or disregarding dissonant elements and adding new consonant elements. It is concluded that, in this context, the aspiration for adopting the figure of the judge of guarantees and of prevention as a cause of exclusion of jurisdiction is justified. And while bills are underway attempting to implement such innovations, judges need to be aware of said phenomenon in order to try to reduce the chances of falling into the pitfalls of their minds. The study conducted is of an exploratory-comprehensive, legal-dogmatic nature, giving priority for content analysis.*

Keywords: *Criminal Procedure Law; Social Psychology; Cognitive dissonance; Criminal justice decision-making; Effects.*

Introdução

Todas as pessoas querem ser coerentes em suas atitudes, opiniões, crenças e comportamentos. Ninguém quer expressar posições contraditórias e inconsistentes, que deixam o indivíduo numa posição desconfortável, fazendo com que aja tentando manter a coerência entre suas convicções e suas atitudes.

Também os juízes querem ser coerentes e consistentes em suas crenças, ações e pronunciamentos, mas, como seres humanos que são, estão sujeitos a limitações e a paixões que podem comprometer a realização da justiça. Naturalmente, eles não estão isentos de, consciente ou inconscientemente, tomarem decisões falhas, preconceituosas e injustas.

O pronunciamento judicial desacertado pode decorrer da má interpretação da lei ou da equivocada valoração das provas encartadas nos autos. Mas o provimento defeituoso, que se distancia do ideal de justiça, pode também ser fruto dos efeitos da denominada dissonância cognitiva, um fenômeno psicológico que há muito foi identificado por Leon Festinger, estudioso da área da psicologia social. Trata-se de angústia ou desconforto mental experimentado pelo tomador da decisão que se vê diante de duas cognições (convicções ou opiniões) contraditórias. Essas cognições dissonantes (discrepantes) acarretam um estado de tensão por ele não querer abandonar uma crença primeva, mas também por não querer parecer incoerente[2].

Assim, neste trabalho, pretende-se abordar a dissonância cognitiva, analisando como ela pode impactar na tomada da decisão judicial na esfera criminal. Como seus efeitos podem refletir na tomada da decisão no âmbito do processo penal? Também se almeja comentar sobre o anseio pela adoção da figura do juiz de garantias e da regra de prevenção como causa de exclusão da competência, assim como a premente necessidade de os magistrados terem clara consciência do fenômeno em estudo.

O tema em questão, portanto, revela-se de fundamental importância para o ofício judicante e atualmente não pode ser ignorado por nenhum magistrado e nem pelos demais profissionais do direito.

---

[2] FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. de Eduardo Almeida. Rio de Janeiro: Zahar Editores, 1975, p. 13.

1. A teoria da dissonância cognitiva

A psicologia social é a área da psicologia que estuda como as influências sociais moldam o comportamento humano; é o ramo da psicologia que investiga como os indivíduos pensam, veem e influenciam uns aos outros[3].

A dissonância cognitiva, por sua vez, é um dos assuntos mais estudados na psicologia social, a partir de pesquisa científica pioneira, realizada em meados dos anos 50, por Leon Festinger, professor de psicologia social da Universidade de Stanford.

O ser humano naturalmente possui ideias ou cognições que são consonantes (coerentes, compatíveis ou correspondentes), assim como pode ter opiniões ou convicções dissonantes (incoerentes, incompatíveis ou discordantes) entre dois conjuntos de elementos[4].

Festinger centrou seus estudos exatamente na tensão ou angústia psicológica que uma pessoa sente ao tomar consciência de que possui pensamentos ou crenças contraditórias (dissonantes) sobre algum elemento relevante, quando percebe que tem opiniões (cognições) discrepantes acerca de algum assunto de maior importância. Esse desconforto foi denominado de dissonância cognitiva[5].

A coerência consigo mesmo e também com os outros é um sentimento que as pessoas valorizam muito. Por isso, quando suas ideias, sentimentos ou comportamentos entram em conflito, mostram-se incompatíveis, elas se sentem desconfortáveis, vivem uma situação de tensão decorrente da falta de harmonia (dissonância) entre dois pensamentos ou crenças relevantes.[6] O grau ou magnitude da dissonância dependerá da maior importância ou do valor dos elementos cognitivos em contraste.

---

[3] MYERS, David G. *Psicologia Social.* 10ª ed. Trad. de Daniel Bueno, Maria Cristina Monteiro e Roberto Cataldo Costa. Rio de Janeiro: AMGH Editora, 2014, p. 28.

[4] FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. de Eduardo Almeida. Rio de Janeiro: Zahar Editores, 1975, p. 12 e 18.

[5] FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. de Eduardo Almeida. Rio de Janeiro: Zahar Editores, 1975, p. 13.

[6] FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. de Eduardo Almeida. Rio de Janeiro: Zahar Editores, 1975, p. 11-15.

A dissonância cognitiva pode decorrer da inconsistência lógica entre duas ideias, pode advir de hábitos culturais diversos, da defesa de opiniões ou posições antagônicas ou ser reflexo de uma experiência passada[7]. Surgirá no momento em que a pessoa ficar consciente de suas duas cognições relevantes e discrepantes.

A teoria revela que "a existência de dissonância origina pressões para reduzi-la e para evitar o seu recrudescimento. As manifestações da operação dessas pressões incluem mudanças de comportamento, mudanças de cognição e busca de novas informações"[8]. O ser humano modifica suas ações ou atitudes e adiciona seletivamente novas informações com o propósito de tentar manter a consistência, buscando atingir a coerência entre suas cognições conflitantes.

Além de pesquisas comportamentais, já há estudos de neurociência[9] que, por meio do exame de imagens do cérebro, buscam analisar a atividade mental do indivíduo antes e depois da decisão geradora da dissonância cognitiva. Conquanto não desvendem os mecanismos neuro-cognitivos que impulsionam a mudança de atitude, os achados das pesquisas mostram que acontecem rapidamente e sem intenção explícita as ativações neurais que levam à mudança de atitude, justamente para fazer cessar o sofrimento psicológico.

A teoria da dissonância cognitiva, portanto, evidencia que o indivíduo modifica ou ajusta seu pensamento ou sua atitude com o propósito de manter a coerência entre suas cognições ou crenças contraditórias, afastamento a tensão psíquica que lhe gera incômodo ou angústia. A busca por consonância, a tentativa de reconciliar cognições discrepantes é um anseio básico, natural do ser humano[10].

---

7 FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. de Eduardo Almeida. Rio de Janeiro: Zahar Editores, 1975, p. 22-23.

8 FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. de Eduardo Almeida. Rio de Janeiro: Zahar Editores, 1975, p. 22-23.

9 BERKMAN, Elliot T.; JARCHO, Johanna M.; LIEBERMAN, Matthew D. *The neural basis of rationalization*: cognitive dissonance reduction during decision-making. SCAN (2011) 6, p. 460–467. Published by Oxford University Press. doi:10.1093/scan/nsq054. Acesso em 25 ago. 2019.

10 FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. de Eduardo Almeida. Rio de Janeiro: Zahar Editores, 1975, p. 13.

Porém, o que Festinger descobriu — e acabou por tornar sua pesquisa tão marcante — é que a pessoa procura eliminar ou diminuir a dissonância mais pela mudança de atitudes pessoais do que pelo abandono da crença ou da opinião anterior.[11] O indivíduo passa a buscar, de modo seletivo, informações correspondentes ou consonantes à sua crença, à sua primeira ação ou decisão.

Dois exemplos ajudarão a bem compreender a dissonância cognitiva. O primeiro, trazido por Festinger, é o do fumante habitual que é alertado para o fato de que o tabaco é mau para a sua saúde[12]:

> Esse conhecimento é certamente dissonante com a cognição de que continua a fumar. Se estiver certa a hipótese de que haverá pressões para reduzir essa dissonância, o que se esperaria que essa pessoa faça? 1. Ela poderá simplesmente mudar a sua cognição sobre o seu comportamento modificando as suas ações; isto é, poderá deixar de fumar. Se já não fuma mais, então a sua cognição do que faz é consonante com o seu conhecimento de que o fumo é nocivo à saúde. 2. Ela poderá mudar os seus 'conhecimentos' sobre os efeitos do fumo. Isso parece ser uma forma algo peculiar de expressá-lo, mas traduz perfeitamente o que deve acontecer. A pessoa talvez acabe por acreditar, simplesmente, que o fumo não tem quaisquer efeitos deletérios ou por adquirir tantos 'conhecimentos' sobre os bons efeitos do fumo que os aspectos nocivos tornar-se-ão desprezíveis. Se conseguir mudar o seu conhecimento de uma ou outra dessas maneiras, terá reduzido, ou mesmo eliminado, a dissonância entre o que faz e o que sabe.

Esse exemplo de Festinger depois ensejou alguns experimentos justamente com fumantes. Aronson, Wilson e Akert[13] mencionam o caso dos fumantes inveterados que buscaram tratamento para abandonar o vício, deixaram o cigarro por um tempo, mas depois voltaram a

---

[11] FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. de Eduardo Almeida. Rio de Janeiro: Zahar Editores, 1975, p. 70-80.

[12] FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. de Eduardo Almeida. Rio de Janeiro: Zahar Editores, 1975, p. 15.

[13] ARONSON, Elliot; WILSON, Timothy D.; AKERT, Robin M. *Psicologia Social*. 3ª ed. Trad. de Ruy Jungmann. Rio de Janeiro: LTC, 2002, p. 115 e 116.

fumar intensamente, passando a minimizar os perigos do tabaco. Eles tinham ciência dos riscos inerentes à prática, isto é, sabiam que poderiam morrer prematuramente por conta de um câncer e que o mais coerente a fazer era mesmo deixar de fumar. Todavia, como cederam ao vício, para diminuir a dissonância, buscaram convencer-se de que fumar não era assim tão nocivo à saúde, passando a apresentar desculpas diversas para se justificar, dizendo, por exemplo, que os estudos sobre o câncer não eram conclusivos, que o filtro do cigarro retinha grande parte da nicotina ou que conheciam uma pessoa bem idosa que fumava desde a juventude[14].

O segundo exemplo é fornecido David Myers[15], ao narrar que parte dos norte-americanos considerava que a guerra do Iraque, em 2003, era justificada para que aquele país, comandado por Saddam Hussein, não fizesse uso de armas de destruição em massa. Mas, depois, quando tais armas não foram encontradas, "a maioria favorável à guerra experimentou dissonância, a qual foi intensificada por sua consciência dos custos financeiros e humanos da guerra". Os apoiadores do conflito reviram seus argumentos e passaram a sustentar que "as razões tornaram-se libertar um povo oprimido do governo tirânico e genocida e estabelecer as bases para um Oriente Médio mais pacífico e democrático".

Ao longo dos anos, a partir das ideias iniciais de Festinger, vários outros estudos e experimentos foram feitos sobre a temática, mas prevalece a concepção original reveladora de que os seres humanos se valem de diversas estratégias para remover ou diminuir a dissonância cognitiva, pois ninguém quer parecer incoerente ou inconsistente[16]. As pessoas buscam novas informações e simulam atitudes não só para diminuir ou eliminar o desconforto (dissonância) e justificar suas crenças

---

[14] ARONSON, Elliot; WILSON, Timothy D.; AKERT, Robin M. *Psicologia Social*. 3ª ed. Trad. de Ruy Jungmann. Rio de Janeiro: LTC, 2002, p. 116.

[15] MYERS, David G. *Psicologia Social*. 10ª ed. Trad. de Daniel Bueno, Maria Cristina Monteiro e Roberto Cataldo Costa. Rio de Janeiro: AMGH Editora, 2014, p. 126.

[16] HARMON-JONES, Eddie; HARMON-JONES, Cindy. Cognitive dissonance theory after 50 years of development. *Zeitschrift für Sozialpsychologie, 38*(1), 2007, p. 13. http://dx.doi.org/10.1024/0044-3514.38.1.7. Acesso em 15 mar. 2019.

e atos, mas também visando a preservar ou a manter sua autoimagem positiva ou sua autoestima[17].

Como se vê, a mudança de atitude ou de comportamento pode expressar-se de diversas formas. A pessoa pode, diante de uma situação de dissonância cognitiva, alterar seus argumentos, tentando manter a consistência entre as opiniões contraditórias, assim como pode ignorar elementos cognitivos dissonantes. Pode adicionar (seletivamente) mais informações, tentando aumentar o número de elementos cognitivos consonantes que justifiquem sua ação e reduzam a dissonância. Pode, também, praticar um ato ou expressar uma ideia que não condiz com sua crença ou ideia tão somente para afastar a tensão entre suas duas cognições incompatíveis[18]. Noutras palavras, a pessoa pode alinhar ou ajustar suas atitudes em conformidade com seus comportamentos anteriores, de modo a buscar coerência e a poder justificar seus atos ou escolhas.

Essa breve explanação é suficiente para apresentar a essência dessa teoria de que o ser humano age para reduzir ou eliminar a dissonância que sente quando tem duas opiniões (cognições) contraditórias. Parece nítido como esse fenômeno influencia ou distorce o processo de tomada de decisão. A necessidade de manter a coerência e preservar a autoimagem gera atitudes que nem sempre são as mais racionais ou revelam comportamentos simulados, marcados pela insinceridade ou hipocrisia[19].

O certo é que a teoria desenvolvida por Festinger desvela que quanto mais comprometido se está com uma ideia ou crença, mais difícil é abandoná-la, mesmo que surjam evidências fortes em sentido contrário. Ainda que sejam confrontadas as razões que levaram a uma decisão, a pessoa tende a apresentar novas informações justificadoras de seu agir ou pensar. Cabe aqui lembrar uma máxima de Pensées Joubert, pensador

---

17 GLEITMAN, Henry; FRIDLUND, Alan J.; REISBERG, Daniel. *Psicologia*. 6ª ed. Trad. de Danilo R. Silva. Lisboa: Fundação Calouste Gulbenkian, 2003, p. 615.

18 DAVIDOFF, Linda L. *Introdução à Psicologia*. 3ª ed. Trad. de Lenke Peres. São Paulo: Pearson Madron Books, 2001, p. 360.

19 MYERS, David G. *Psicologia Social*. 10ª ed. Trad. de Daniel Bueno, Maria Cristina Monteiro e Roberto Cataldo Costa. Rio de Janeiro: AMGH Editora, 2014, p. 126.

francês citado por Myers[20], alertando para o fato de que "aqueles que nunca voltam atrás em suas opiniões amam mais a si mesmos do que à verdade".

No tópico seguinte, almeja-se expor como o fenômeno da dissonância cognitiva pode influenciar diretamente a tomada de decisões judiciais na seara penal.

2. A dissonância cognitiva e seus reflexos na tomada da decisão judicial criminal

É relevante e crescente o interesse em entender, à luz da psicologia cognitiva e da neurociência, como o juiz, valendo-se de heurísticas, age e pensa para resolver problemas e tomar decisões, estando sujeito a falhas ou vieses[21]. O entusiasmo pela compreensão desses processos mentais aumenta quando se nota, a partir da psicologia social e da teoria da dissonância cognitiva, que o desejo de manter a coerência e a preocupação com a autoimagem podem influenciar a tomada de decisão por parte do julgador.

A dissonância cognitiva, definida como o desconforto ou tensão gerada a partir de duas crenças ou cognições contraditórias, não é um fenômeno atípico na vida dos juízes. Como proferem inúmeras decisões em suas jornadas, é normal e até comum que haja pontos de tensão entre os entendimentos que expressam em diversos casos, por suas peculiaridades, e também no curso de um mesmo processo.

Segundo Ruiz Ritter[22], a teoria da dissonância cognitiva evidencia que todo o indivíduo tende a buscar um estado de coerência entre suas crenças, pensamentos e atitudes, de forma que, quando se vê diante de cognições discrepantes, passa a enfrentar uma situação incômoda,

---

[20] MYERS, David G. *Psicologia Social.* 10ª ed. Trad. de Daniel Bueno, Maria Cristina Monteiro e Roberto Cataldo Costa. Rio de Janeiro: AMGH Editora, 2014, p. 178.

[21] ANDRADE, Flávio da Silva. A tomada da decisão judicial criminal à luz da psicologia: heurísticas e vieses cognitivos. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 1, p. 507-540, jan./abr. 2019. https://doi.org/10.22197/rbdpp.v5i1.172. Acesso em 15 mar. 2019.

[22] RITTER, Ruiz. *Imparcialidade no processo penal*: reflexões a partir da teoria da dissonância cognitiva. Florianópolis: Empório do Direito, 2017, p. 162.

desconfortável, de tensão psicológica, responsável pela manifestação de diversos processos involuntários direcionados a restabelecer a harmonia interna entre suas crenças, opiniões e comportamentos. "Logo, pode-se afirmar que há uma tendência, no ser humano, à estabilidade cognitiva, intolerante a incongruências, que são inevitáveis nos casos de tomada de decisões (...)".

Algumas ilustrações auxiliarão a entender como a tensão psicológica entre duas crenças ou cognições contraditórias pode fazer com que um juiz aja, instintivamente[23], tentando eliminar ou diminuir a dissonância mais pela mudança de atitude ou de comportamento do que pelo abandono da crença ou opinião anterior.

Há flagrante dissonância quando o julgador, em sede de cognição sumária[24], ao analisar uma medida de urgência, faz um juízo positivo da probabilidade do direito alegado, mas depois, no juízo de cognição exauriente, constata que não existe o direito afirmado. Mesmo que o primeiro juízo tenha sido de mera probabilidade (e não de certeza), o magistrado, dependendo da hipótese, sentirá certo desconforto por ter reconhecido a plausibilidade de um direito inexistente.

Por exemplo, se o juiz, na fase investigativa, entendendo presentes os pressupostos (prova da materialidade delitiva e indícios de autoria) e um dos fundamentos da prisão preventiva, como a necessidade de garantir a ordem pública, vem a decretar a custódia preventiva de um acusado, tende a sentir algum desconforto ou angústia para depois admitir que

---

[23] Como assinalou Enrico Altavilla: "Não é somente com as faculdades intelectuais que o homem julga, mas também com suas faculdades instintivas, com os seus sentimentos (...). O instinto é, na verdade, um fator obscuro e poderoso de todo julgamento, e principalmente do que é feito pelo magistrado penal. (...) No julgamento penal têm, frequentemente, predomínio certos movimentos sentimentais e emotivos, que dão uma orientação especial à personalidade do juiz que procede ao exame das provas" (ALTAVILLA, Enrico. *Psicologia Judiciária*. Personagens do processo penal. Vol. V. 4ª ed. Trad. de Fernando de Miranda. Coimbra: Armênio Amado, 1960, p. 66-67).

[24] Quanto ao grau de profundidade do conhecimento do juiz, ou seja, quanto à abrangência vertical com que o magistrado analisa os fatos, a cognição pode ser superficial (conhecimento sem profundidade, mero juízo de probabilidade) ou exauriente (conhecimento integral das provas para resolver a questão) (GAGLIARDI, Pedro. *As liminares em processo penal*. São Paulo: Saraiva, 1999, p. 22).

a conduta era atípica ou que os indícios que justificaram a prisão por razoável período são frágeis e não permitem a condenação.

Numa outra hipótese, o magistrado que deferiu pleitos de interceptação telefônica e de prorrogação dessas escutas se mostra mais propenso a receber a denúncia atinente aos fatos investigados. Se admitiu o emprego de referida medida mais invasiva de apuração, é difícil ele não reputar presentes elementos bastantes para o início da ação penal. Do mesmo modo, o juiz que rejeitou pedidos de quebras de sigilo (bancário e fiscal) tende a ser mais rigoroso no exame da admissibilidade da peça acusatória.

Pode haver dissonância cognitiva quando o juiz, a partir do que decidiu em sede de cognição sumária (superficial), no início da lide, depara-se depois, ao final, na cognição exauriente (completa ou exaustiva), com evidências ou elementos diversos que não corroboram a avaliação inicial. O magistrado pode ficar inclinado a agir para confirmar o conteúdo da decisão produzida em cognição sumária. Por causa do *lock-in effect* (viés de trancamento), estará mais propenso a manter a decisão anterior, ainda que tenha sido tomada sem uma cognição plena da questão, já que antes investiu tempo e pesquisa, firmando uma convicção sobre o assunto. O juiz pode tender a decidir de forma a "demonstrar racionalidade com relação ao seu próprio raciocínio ou restaurar a consistência entre as consequências de suas ações e seu conceito próprio de tomada de decisão racional"[25].

Entrementes, o juízo provisório evidentemente não pode se sobrepor ou definir os rumos dos juízos definitivos. Da parte do tomador da decisão, é preciso muito cuidado para esse ponto, pois a ingerência do primeiro juízo sobre o segundo acontece também por força de estímulos que estão abaixo do nível da consciência.

Ao comentar sobre a dissonância pós-primeira impressão, Ritter[26] aduziu o seguinte:

---

[25] LYNCH, Kevin J. The lock in effect of preliminary injunctions. *Florida Law Review*. Vol. 66, 2014, p. 785. Disponível em: <http://www.floridalawreview.com/wp-content/uploads/9-Lynch.pdf>. Acesso em 28/09/2019.

[26] RITTER, Ruiz. *Imparcialidade no processo penal*: reflexões a partir da teoria da dissonância cognitiva. Florianópolis: Empório do Direito, 2017, p. 144.

> "(...) após a obtenção de uma cognição inicial (primeira impressão) sobre alguém (positiva ou negativa), a tendência do indivíduo é de preservá-la, evitando-se o rompimento do seu estado de consonância cognitiva, que somente estará em perigo se esta for contrariada. Não sendo possível, porém, dita manutenção, sobrevindo cognições que questionam aquela primeira (novas informações aptas a modificarem a primeira impressão), entrarão em cena processos involuntários destinados ao restabelecimento do *status quo*. São eles a mudança de elementos cognitivos envolvidos em relações dissonantes; a desvalorização de elementos cognitivos envolvidos em relações dissonantes; a adição de novos elementos cognitivos que sejam consonantes com a cognição existente; e a evitação ativa do aumento desses elementos dissonantes, além das três técnicas especificas da percepção errônea, da invalidação e do esquecimento seletivo".

De outro lado, quando compara os casos similares que lhe são submetidos, mas entende que, por alguma especificidade, merecem soluções diversas, o magistrado também experimenta dissonância cognitiva e busca explicitar aspectos das causas e argumentos que justifiquem as resoluções em sentidos diferentes, em vista do desejo de decidir cada disputa de forma consistente, com acerto e justiça. O juiz, até porque quer guardar coerência com sua posição acerca da matéria, tende a relutar para decidir[27] de forma diferente do que fez no processo antecedente.

Ainda, acaso o juiz rejeite a peça inicial acusatória, por entender que inexiste justa causa para a abertura do processo, vindo a segunda instância a dar provimento ao recurso do Ministério Público, recebendo a denúncia, pode depois aquele julgador de 1º grau, de modo enviesado, apresentar resistência para condenar o réu, ainda que a acusação exiba

---

[27] Ruiz Ritter, ao refletir sobre a imparcialidade e os impactos da dissonância cognitiva no processo penal, afirma que "*decidir* não é apenas fazer uma escolha. Muito mais do isso, é assumir (fiel e involuntariamente) o compromisso de conservar uma posição, que decisivamente vinculará o seu responsável por prazo indeterminado, já que tudo que a contrariar produzirá dissonância e deverá ser evitado, ou se não for possível, deturpado" (RITTER, Ruiz. *Imparcialidade no processo penal*: reflexões a partir da teoria da dissonância cognitiva. Florianópolis: Empório do Direito, 2017, p. 133).

provas bastantes de sua culpa. Da mesma forma, se a defesa obtiver a anulação da sentença condenatória por cerceamento na sua atuação, o magistrado que condenou o réu na primeira instância, se tiver de novamente julgar o caso, estará mais propenso a proferir novo édito condenatório, se não policiar seu proceder[28], se não atentar para o fenômeno psicológico aqui debatido.

Já o magistrado que sustenta certa posição numa obra acadêmica ou num discurso sentirá dissonância se, num caso concreto submetido à sua análise, tiver de assumir posição diversa, de forma que pode se ver mudando ou simulando atitudes com o propósito de diminuir ou eliminar o desconforto (dissonância). Se não ficar atento, sucumbirá à pressão voltada ao estabelecimento de correspondência entre os elementos cognitivos, podendo o caso reclamar solução diversa.

Mais um e último exemplo de situação em que pode acontecer o fenômeno da dissonância cognitiva: se, num colegiado, o relator é surpreendido por um excelente voto-vista em sentido contrário a seu encaminhamento para o caso, sentirá enorme desconforto, mas resistirá para mudar sua posição, ainda que sejam muito sólidos e precisos os argumentos contrários apresentados pelo juiz que depois dele veio a votar. É natural que assim aconteça por uma questão de autoestima, de preservação da autoimagem.

Comentando sobre como decidem os tribunais brasileiros, José Rodrigo Rodriguez[29] afirma que o desenho do Poder Judiciário pode refletir sobre os efeitos de julgamentos colegiados ou singulares no que tange à congruência das decisões. Rodriguez[30] esclarece que:

---

[28] Os sentimentos, a emoção e a intuição (arquétipo da *anima*) naturalmente têm valor no processo de tomada de decisão judicial, mas a racionalidade jamais pode ser abandonada. O uso equilibrado dessas ferramentas pelo magistrado é que conduzem à solução mais justa e adequada da demanda (PRADO, Lídia Reis de Almeida. Racionalidade e emoção na prestação jurisdicional. In: ZIMERMAN, David; COLTRO, Antônio Carlos Mathias (Orgs.). *Aspectos psicológicos da atividade jurídica*. 3ª ed. Campinas: Millennium, 2002. p. 91-93).

[29] RODRIGUEZ, José Rodrigo. Como decidem as cortes?: para uma crítica do direito (brasileiro). Rio de Janeiro: Editora FGV, 2013, p. 155.

[30] RODRIGUEZ, José Rodrigo. Como decidem as cortes?: para uma crítica do direito (brasileiro). Rio de Janeiro: Editora FGV, 2013, p. 155.

> "Há pesquisas cujo objetivo é averiguar empiricamente a variação no resultado destes dois modos de desenhar os organismos jurisdicionais. Uma delas (Schauer e Zeckhauser, 2007) aponta que em julgamentos colegiados corre-se o risco de que o debate entre os juízes roube a cena em detrimento das circunstâncias do caso concreto. Torna-se mais importante vencer o oponente do que resolver o problema apresentado aos juízes".

As transmissões, ao vivo, das sessões Corte Suprema brasileira pela televisão ou pela *internet* permitem notar com clareza como amiúde acontecem tais embates. O colegiado deveria funcionar como um filtro corretivo de posições ou de eliminação de vieses cognitivos, mas a perseverança da crença se faz ali presente e os julgadores tentam evitar que sejam vistos como tomadores de decisões inconsistentes. Abraçados a sua solução egoísta[31], agem mais preocupados em apresentar ao público uma imagem positiva de si mesmos[32]. Os longos votos escritos também se tornam formas de buscar a redução da dissonância (também notada pelo público externo), reafirmar posições preconcebidas e tentar evitar danos à reputação da justiça.

Destarte, muitas vezes, o comprometimento prévio com uma posição faz com que o julgador tenha dificuldade de acompanhar a maioria num colegiado[33], de voltar atrás numa decisão ou de julgar em sentido contrário à ideia inicial. É assim também quando se assume um compromisso público, em que se costuma ficar preso a uma declaração ou

---

[31] O fato de os ministros muitas vezes levarem votos prontos, escritos, parece dificultar para que eles concordem com seus pares a partir da força e da pertinência de seus argumentos e ponderações. Costuma prevalecer a crença ou o entendimento com o qual cada um já está psicologicamente comprometido.

[32] COLLINS Jr, Paul M. Cognitive Dissonance On The U.S. Supreme Court. *Workshop On Law, Economics, And Politics, University Of Texas School Of Law*,February 2, 2009, p. 6-8. Disponível em:<https://law.utexas.edu/wp-content/uploads/sites/25/collins_cognitive_dissonance.pdf>. Acesso em 28 set. 2019.

[33] "Quando o plenário decide e o ministro-agente discorda, usa o poder de decisão monocrática para ignorar ou contrariar a manifestação do plenário. Mesmo vencido no colegiado, o ministro continua a promover sua posição, agora jogando sozinho" (FALCÃO, Joaquim; Arguelhes, Diego Werneck. Onze Supremos, todos contra o plenário. In: Falcão, Joaquim; Arguelhes, Diego; Recondo, Felipe (Orgs.). *Onze supremos*: o supremo em 2016. Belo Horizonte: Letramento; Casa do Direito; Supra; Jota; FGV Rio, 2017, p. 23-24).

uma compreensão sobre determinado tema, de maneira que a persuasão ficará restringida, hesitando-se muito para reverter um ponto de vista.

Nesses casos, à luz da teoria da dissonância cognitiva, o juiz pode ficar apegado à crença ou à opinião anterior, vindo a praticar ato ou a expressar ideias que não condizem com seu pensamento apenas para afastar a tensão entre as duas cognições contraditórias. Pode querer adicionar informações, ajustar sua compreensão e agir consoante seu entendimento anterior tão somente para manter a consistência e a coerência entre seus atos, preservando sua autoimagem.

Bernd Schünemann[34] vai além, não se detendo nas possibilidades acima comentadas e que rodeiam o raciocínio judicial. Para o professor alemão, a dissonância cognitiva efetivamente produz o efeito perseverança ou o mecanismo de autoafirmação, assim como leva inevitavelmente à busca seletiva de informações:

> "O efeito perseverança ou inércia ou mecanismo de autoafirmação da hipótese preestabelecida faz com que as informações, previamente consideradas corretas à ratificação da hipótese preconcebida, sejam sistematicamente superestimadas, enquanto que as informações dissonantes sejam sistematicamente subavaliadas. Já o princípio da busca seletiva de informações favorece a ratificação da hipótese originária que tenha sido, na autocompreensão individual, aceita pelo menos uma vez. Isso ocorre pelo condicionamento da busca à obtenção de informações que confirmem a preconcepção, o que pode se dar tanto pela coleta de informações em consonância com a hipótese, quanto pela de informações dissonantes facilmente refutáveis (...)".

Em verdade, no contexto da dissonância cognitiva, faz-se muito presente o viés de confirmação (*confirmation bias*), falha cognitiva daquele que, devendo justificar uma determinada escolha, seleciona apenas os elementos ou evidências que confirmam sua correção, ignorando os fatores contrários[35]. Muitas vezes, "após uma decisão, registra-se uma

---

[34] SCHÜNEMANN, Bernd. O juiz como um terceiro manipulado no processo penal? Uma confirmação empírica dos efeitos perseverança e correspondência comportamental. *Revista Liberdades*, São Paulo, n. 11, set./dez. 2012, p. 35.

[35] Para uma abordagem detalhada do assunto: TABAK, Benjamin Miranda; AGUIAR, Julio Cesar; NARDI, Ricardo Perin. O viés confirmatório no

busca ativa de informações que produzam uma cognição consonante com a ação empreendida"[36].

Assim, se não tiver consciência do fenômeno em questão, o juiz pode deixar que a compreensão firmada num primeiro momento influencie naquilo que será decidido de forma definitiva naquele processo, ainda que as provas amealhadas caminhem em sentido diverso. A presença da dissonância leva à busca de informações correspondentes à primeira decisão.

A cognição sumária é essencial para resguardar a utilidade do provimento final e também para assegurar o gozo do direito numa situação de urgência, mas ela não pode definir o fundo do direito[37], tarefa que deve ser cumprida pela cognição exauriente. Como o juiz não é uma máquina[38], o trabalho feito em sede de cognição sumária acaba por influenciar — e isso é natural — a formulação da cognição plena, mas jamais pode determinar o resultado do processo. Se ele ficar vinculado a sua pré-compreensão, olvidando que decidiu com base na aparência do direito alegado, num momento em que o acusado não teve chance de se manifestar, desprezando completamente suas provas, não julgará com imparcialidade.

Lucas Theodoro Dias Vieira e Natanael Lud Santos e Silva[39] bem detectaram o problema em foco:

---

argumento probatório e sua análise através da inferência para melhor explicação: o afastamento do decisionismo no processo penal. *Revista da Faculdade de Direito da UFMG*. Belo Horizonte, n. 70, jan/jun. 2017, p. 184-185. https://doi.org/10.12818/P.0304-2340.2017v70p177

36 FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. de Eduardo Almeida. Rio de Janeiro: Zahar Editores, 1975, p. 80.

37 RAMOS, João Gualberto Garcez. *A tutela de urgência no processo penal brasileiro*. Belo Horizonte: Del Rey, 1998, p. 88.

38 Vale assinalar que os traços caracterológicos do juiz, seu perfil psicológico, seus valores pessoais, quer seja de ordem moral, política, religiosa, social, cultural, científica ou ética, constituem fatores que influenciam, consciente ou inconscientemente, a tomada da decisão judicial (ZIMERMAN, David. A influência dos fatores psicológicos inconscientes na decisão jurisdicional: a crise do magistrado. In: ZIMERMAN, David; COLTRO, Antônio Carlos Mathias (Orgs.). *Aspectos psicológicos da atividade jurídica*. 3ª ed. Campinas: Millennium, 2002, p. 125-132).

39 VIEIRA, Lucas Theodoro Dias, SILVA, Natanael Lud Santos e. O modelo atitudinal de julgamento, os vieses de cognição e a colegialidade corretiva: Breves considerações. In: *Direito na Atualidade:* Uma Análise Multidisciplinar. André

> "Portanto, em especial no tocante à vinculação com as decisões liminares, quando se trata das chamadas tutelas de urgência (inclusive os habeas corpus), também a "Teoria da Dissonância Cognitiva" vem reforçar o entendimento de que é necessário um movimento de contrapeso à costumeira tendência de forma atitudinal de julgamento nos Tribunais, de modo a impedir que as influências metajurídicas que os magistrados sobem sejam estímulos para decisões desrespeitosas a um modelo constitucional e comparticipativo de processo".

Por conseguinte, é a partir da referida teoria da dissonância cognitiva que se tem defendido, de maneira consistente e fundamentada, a adoção, pelo ordenamento jurídico-penal brasileiro, da figura do juiz de garantias[40]

Vicente Leite de Freitas, Fernanda Paula Diniz, Henrique Viana Pereira (Organizadores). Rio de Janeiro: Lumen Juris, 2016, p. 95.

[40] No projeto de lei do novo Código de Processo Penal (Projeto de Lei do Senado nº 156/2009, em trâmite no Congresso Nacional, o juiz de garantias foi assim disciplinado: "Art. 14. O juiz das garantias é responsável pelo controle da legalidade da investigação criminal e pela salvaguarda dos direitos individuais cuja franquia tenha sido reservada à autorização prévia do Poder Judiciário, competindo-lhe especialmente: I – receber a comunicação imediata da prisão, nos termos do inciso LXII do art. 5º da Constituição da República Federativa do Brasil; II – receber o auto da prisão em flagrante, para efeito do disposto no art. 555; III – zelar pela observância dos direitos do preso, podendo determinar que este seja conduzido a sua presença; IV – ser informado sobre a abertura de qualquer investigação criminal; V – decidir sobre o pedido de prisão provisória ou outra medida cautelar; VI – prorrogar a prisão provisória ou outra medida cautelar, bem como substituí-las ou revogá-las; VII – decidir sobre o pedido de produção antecipada de provas consideradas urgentes e não repetíveis, assegurados o contraditório e a ampla defesa; VIII – prorrogar o prazo de duração do inquérito, estando o investigado preso, em vista das razões apresentadas pelo delegado de polícia e observado o disposto no parágrafo único deste artigo; IX – determinar o trancamento do inquérito policial quando não houver fundamento razoável para sua instauração ou prosseguimento; X – requisitar documentos, laudos e informações ao delegado de polícia sobre o andamento da investigação; XI – decidir sobre os pedidos de: a) interceptação telefônica, do fluxo de comunicações em sistemas de informática e telemática ou de outras formas de comunicação; b) quebra dos sigilos fiscal, bancário e telefônico; c) busca e apreensão domiciliar; d) acesso a informações sigilosas; e) outros meios de obtenção da prova que restrinjam direitos fundamentais do investigado. XII – julgar o habeas corpus impetrado antes do oferecimento da denúncia; XIII – determinar a realização de exame médico de sanidade mental, nos termos do art. 452, § 1º; XIV – arquivar o inquérito policial; XV – assegurar

e da prevenção[41] como causa de exclusão da competência, de forma a se evitar decisões enviesadas ou falhas.

Aury Lopes Jr. e Ruiz Ritter asseveram que o acesso aos autos do inquérito policial e a tomada de decisões na fase de investigação preliminar podem vincular cognitivamente o juiz, pois ele, natural e inconscientemente, depois sentirá a necessidade de manter a coerência com as informações recebidas e com as escolhas feitas na fase preliminar, o que evidencia, em definitivo, "(...) a necessidade de implantação do juiz das garantias, sob pena de não haver sequer condições para o exercício de uma jurisdição imparcial"[42].

---

prontamente, quando se fizer necessário, o direito de que tratam os arts. 11 e 37; XVI – deferir pedido de admissão de assistente técnico para acompanhar a produção da perícia; XVII – outras matérias inerentes às atribuições definidas no caput deste artigo. (...) Art. 15. A competência do juiz das garantias abrange todas as infrações penais, exceto as de menor potencial ofensivo e cessa com a propositura da ação penal. § 1º Proposta a ação penal, as questões pendentes serão decididas pelo juiz do processo. § 2º As decisões proferidas pelo juiz das garantias não vinculam o juiz do processo, que, após o oferecimento da denúncia, poderá reexaminar a necessidade das medidas cautelares em curso. § 3º Os autos que compõem as matérias submetidas à apreciação do juiz das garantias serão apensados aos autos do processo. Art. 16. O juiz que, na fase de investigação, praticar qualquer ato incluído nas competências do art. 14 ficará impedido de funcionar no processo, observado o disposto no art. 748. Art. 17. O juiz das garantias será designado conforme as normas de organização judiciária da União, dos Estados e do Distrito Federal (BRASIL. Senado Federal. Projeto de Lei nº 156/2009. Dispõe sobre a reforma Código de Processo Penal. Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/90645>. Acesso em: 27 set. 2019).

41 Segundo Gustavo Badaró, ''prevenção vem do latim *prae-venire*, que significa chegar antes." No código em vigor, a prevenção enseja a "concentração, em um órgão jurisdicional, da competência que abstratamente pertencia a mais de um órgão, inclusive a ele próprio, por ter atuado, previamente, no processo" (BADARÓ, Gustavo Henrique. **Processo Penal.** 6ª ed. São Paulo: Revista dos Tribunais, 2018, p. 249).

42 LOPES JR., Aury; RITTER, Ruiz. A imprescindibilidade do juiz das garantias para uma jurisdição penal imparcial: reflexões a partir da teoria da dissonância cognitiva. *Revista Magister de Direito Penal e Processual Penal*. Porto Alegre, v. 13, n. 73, ago./set. 2016, p. 19-20.

Ao comentar a regra de prevenção do art. 83 do CPP[43], a juíza federal Danielle Souza de Andrade e Silva[44] afirma que, na fase pré-processual, ao ficar em contato com as fontes de investigação, "com a adoção de medidas cautelares, busca e apreensão, autorização para interceptação telefônica etc.," o magistrado realiza diversos pré-julgamentos, destacando que:

> "E esse mesmo juiz, imbuído naturalmente de ideias pré-concebidas, frutos até de sua perspicácia, formará pré-juízos sobre condutas e pessoas, não sendo conveniente que inicie o processo penal com tal comprometimento subjetivo. E foi justamente essa incompatibilidade psicológica que levou ao descrédito do modelo inquisitivo. O sistema ideal, aquele em que se encontraria o ponto de equilíbrio entre as liberdades individuais e a segurança pública, seria o bifásico, que garantisse a separação de funções: o órgão judicial atuante na instrução preliminar e aquele responsável pelo processamento e julgamento da causa propriamente dita, o garantidor do procedimento investigativo e o efetivamente julgador".

Nessa mesma linha de raciocínio, o magistrado Eduardo José da Fonseca Costa[45], do TRF da 3ª Região, a partir de relevante estudo interseccional entre direito processual, economia e psicologia, considera inadequado ou equivocado, comprometedor da imparcialidade objetiva, "a prolação da sentença penal condenatória pelo mesmo juiz que já apreciara pedido de prisão cautelar ou de concessão de medidas na fase investigativa, como busca e apreensão, interceptação telefônica e quebras de sigilo fiscal e bancário".

---

[43] O art. 83 do CPP dispõe o seguinte: "Verificar-se-á a competência por prevenção toda vez que, concorrendo dois ou mais juízes igualmente competentes ou com jurisdição cumulativa, um deles tiver antecedido aos outros na prática de algum ato do processo ou de medida a este relativa, ainda que anterior ao oferecimento da denúncia ou da queixa (arts. 70, § 3º, 71, 72, § 2º, e 78, II, *c*)."

[44] SILVA, Danielle Souza de Andrade e. *A atuação do juiz no processo penal acusatório*. Incongruências no sistema brasileiro em decorrência do modelo constitucional de 1988. Porto Alegre: Sergio Antonio Fabris, 2005, p. 114.

[45] COSTA, Eduardo José da Fonseca. *Levando a imparcialidade a sério*: proposta de um modelo interseccional entre direito processual, economia e psicologia. Salvador: JusPodivm, 2018, p. 160-161.

A preocupação com os efeitos da dissonância cognitiva, indutora do viés de confirmação, tem levado promotores americanos[46] a buscarem por uma segunda opinião sobre as provas de seus casos. Esse novo olhar tem sido considerado útil para evitar que o promotor subestime o valor exculpatório de uma prova posteriormente descoberta. O olhar de um terceiro não será influenciado pelo desejo de evitar a dissonância cognitiva, prevenindo a acusação de inocentes calcada meramente na perseverança de crença.

A teoria da dissonância cognitiva encerra, pois, sólida base científica para justificar as inovações processuais acima apontadas ante o receio ou o temor de que o julgador que atuou na fase investigatória ou que examinou pleitos cautelares possa não preservar a imparcialidade objetiva para ao final julgar a causa. No entanto, se o atual modelo de organização judiciária brasileiro ou a falta de recursos não permitir substituir o juiz tido por "contaminado", que ao menos seja ele abertamente alertado para o risco de cometer injustiças por não perceber que ficou emocionalmente vinculado a uma pré-compreensão, ao primeiro ponto de vista, mesmo quando depois as evidências amealhadas apontavam no sentido contrário.

Não é o caso de aprofundar, neste ensaio, sobre as temáticas do juiz de garantias e da regra de prevenção[47]. O objetivo primordial desse breve estudo é apontar os efeitos da dissonância cognitiva sobre a tomada de decisão no âmbito do processo penal, mostrando que a teoria de Festinger é constitui alicerce seguro para justificar tais inovações ou tecnologias processuais, mas, enquanto não implementadas, devem os juízes estar atentos para o fenômeno, que pode comprometer a imparcialidade objetiva, a independência e conduzir a decisões falhas, enviesadas, distantes do ideal de justiça. A imparcialidade do juiz — note-se — manifesta-se também "pela independência contra seus próprios reflexos, tendências,

---

[46] BURKE, Alafair S. Improving Prosecutorial Decision Making: Some Lessons of Cognitive Science. *William & Mary Law Review*, Vol. 47, 2006, p. 1621-1622. Disponível em:<https://scholarship.law.wm.edu/wmlr/vol47/iss5/3>. Acesso em: 28 set. 2019.

[47] Para uma análise aprofundada desses assuntos: MAYA, André Machado. *Imparcialidade e Processo Penal:* Da prevenção da competência ao Juiz de Garantias. Rio de Janeiro: Lumen Juris, 2011.

proveitos e receios"[48]. Como asseverou Manuel Pedro Pimentel, "somente o juiz livre, livre de preconceitos, livre de juízos apriorísticos, livre de ideias estereotipadas, livre de injunções facciosas, poderá encontrar a verdade, essa mesma verdade que é a única que nos interessa (...)"[49].

O juiz deve desconfiar de si para bem cumprir sua elevada missão[50]; deve querer alcançar a verdade e a justiça, mas deve fazê-lo com humildade, já que suas convicções, suas ideias preconcebidas já podem estar vulneradas pelos fatos e pelos argumentos de outrem[51]. Se não tiver grandeza e altivez para mudar de compreensão quando necessário, seu provimento pode ficar longe de realizar a justiça.

Enfim, diversos fatores podem influenciar a tomada de uma decisão judicial, podem explicar o comportamento e o raciocínio do julgador, mas, por tudo que se expôs neste estudo, a dissonância cognitiva e seus efeitos não podem ser desprezados, devendo ser investigados por aqueles que se importam com o soerguimento de decisões livres de vícios ou defeitos que não se harmonizam com o paradigma do Estado Democrático de Direito.

Considerações finais

A teoria da dissonância cognitiva revolucionou o conhecimento sobre motivações, atitudes e comportamentos humanos, ajudando a desvendar os processos mentais subjacentes à tomada de decisões.

---

[48] BITTENCOURT, Edgard de Moura. *O juiz*. 3ª ed. Campinas: Millennium, 2002, p. 145.

[49] PIMENTEL, Manoel Pedro. Discurso de posse, em 26/04/1962, no cargo de juiz criminal do Tribunal de Alçada de São Paulo *apud* BITTENCOURT, Edgard de Moura. *O juiz*. 3ª ed. Campinas: Millennium, 2002, p. 141.

[50] Eduardo José da Fonseca Costa propõe que o tomador da decisão empregue a técnica do "advogado do diabo" ou do "considerar o oposto" (COSTA, Eduardo José da Fonseca. *Levando a imparcialidade a sério*: proposta de um modelo interseccional entre direito processual, economia e psicologia. Salvador: JusPodivm, 2018, p. 202).

[51] BITTENCOURT, Edgard de Moura. *O juiz*. 3ª ed. Campinas: Millennium, 2002, p. 144.

O desconforto gerado a partir de duas crenças ou cognições discrepantes é um fenômeno relativamente comum na atuação dos juízes criminais, ante o grande número de decisões que proferem nos diversos processos que conduzem. A dissonância se verifica especialmente quando, num determinado processo, o magistrado emite provimentos em sede de cognição sumária (superficial) e de cognição exauriente (plena).

Se o julgador não tiver consciência desse fenômeno tão estudado no campo da psicologia social, o processo de tomada de decisão pode tornar-se distorcido. A necessidade de o juiz manter a coerência e de preservar a autoimagem perante terceiros gera atitudes que nem sempre são as mais racionais. Seus sentimentos se sobrepõem à racionalidade. Busca seletivamente informações que possam aumentar o número de elementos consonantes que justifiquem sua ação e reduzam a dissonância. Pratica ato ou expressa uma ideia que não condiz com seu pensamento apenas para afastar a tensão entre suas duas cognições contraditórias.

O estudo revelou que, num quadro de dissonância cognitiva, tende a eclodir o viés de confirmação (*confirmation bias*), quando o julgador leva em consideração apenas informações ou provas que confirmem sua crença, sua hipótese (elementos consonantes), desprezando os elementos em sentido contrário (elementos dissonantes).

É nesse contexto que tem ganhado força a ideia de se adotar, no ordenamento jurídico-penal pátrio, o denominado juiz de garantias e também a regra de prevenção como mecanismo de afastamento da competência do magistrado que atuou na fase pré-processual ou que apreciou pleitos cautelares. Embora esses temas não tenham sido o foco central desse ensaio, a teoria da dissonância cognitiva encerra um alicerce epistêmico sólido para que o assunto seja seriamente discutido, de modo a se vencer a resistência dos juízes e dos promotores brasileiros, assim como das entidades a que estão vinculados.

Seja como for, o mais relevante é que os integrantes do Poder Judiciário e os demais atores do processo tenham plena consciência do fenômeno aqui abordado. A dissonância cognitiva não pode impedir que o julgador raciocine de forma imparcial e independente. Tendo conhecimento desse fato, o magistrado precisa agir com cautela e discernimento, desconfiando de si mesmo, para não cair nas armadilhas inconscientemente construídas em sua própria mente.

Em arremate, o juiz não pode ser escravo de suas paixões ou preconcepções, que podem colocar em xeque sua imparcialidade e comprometer o acerto de sua decisão. Para bem exercer a tarefa de julgar, interpretando leis e valorando provas no âmbito do processo penal, o julgador deve primeiro vencer seus preconceitos, questionar suas próprias ideias e conhecer seu próprio íntimo, onde, às vezes, de maneira inconsciente, se formam autocompromissos ou prejulgamentos que podem levar a um provimento distante do ideal de justiça.

Referências

ALTAVILLA, Enrico. *Psicologia Judiciária*. Personagens do processo penal. Vol. V. 4ª ed. Trad. de Fernando de Miranda. Coimbra: Armênio Amado, 1960.

ANDRADE, Flávio da Silva. A tomada da decisão judicial criminal à luz da psicologia: heurísticas e vieses cognitivos. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 1, p. 507-540, jan./abr. 2019. https://doi.org/10.22197/rbdpp.v5i1.172

ARONSON, Elliot; WILSON, Timothy D.; AKERT, Robin M. *Psicologia Social.* 3ª ed. Trad. de Ruy Jungmann. Rio de Janeiro: LTC, 2002.

BERKMAN, Elliot T.; JARCHO, Johanna M.; LIEBERMAN, Matthew D. *The neural basis of rationalization*: cognitive dissonance reduction during decision-making. SCAN (2011) 6, p. 460-467. Published by Oxford University Press. http://dx.doi.org/10.1093/scan/nsq054.

BADARÓ, Gustavo Henrique. Processo Penal. 6ª ed. São Paulo: Revista dos Tribunais, 2018.

BITTENCOURT, Edgard de Moura. *O juiz*. 3ª ed. Campinas: Millennium, 2002.

BURKE, Alafair S. Improving Prosecutorial Decision Making: Some Lessonsof Cognitive Science. *William & Mary LawReview*, Vol. 47, 2006, p. 1587-11633. Disponível em:<https://scholarship.law.wm.edu/wmlr/vol47/iss5/3>.

COLLINS Jr, Paul M. Cognitive Dissonance On The U.S. Supreme Court. *Workshop On Law, Economics, And Politics, University Of Texas School Of Law,*February 2,

2009, p. 1-46. Disponível em:<https://law.utexas.edu/wp-content/uploads/sites/25/collins_cognitive_dissonance.pdf>.

COSTA, Eduardo José da Fonseca. *Levando a imparcialidade a sério*: proposta de um modelo interseccional entre direito processual, economia e psicologia. Salvador: JusPodivm, 2018.

DAVIDOFF, Linda L. *Introdução à Psicologia*. 3ª ed. Trad. de Lenke Peres. São Paulo: Pearson Madron Books, 2001.

FALCÃO, Joaquim; Arguelhes, Diego Werneck. Onze Supremos, todos contra o plenário. In: Falcão, Joaquim; Arguelhes, Diego; Recondo, Felipe (Orgs.). *Onze supremos*: o supremo em 2016. Belo Horizonte: Letramento; Casa do Direito; Supra; Jota; FGV Rio, 2017, p. 20-29.

FESTINGER, Leon. *Teoria da dissonância cognitiva*. Trad. de Eduardo Almeida. Rio de Janeiro: Zahar Editores, 1975.

GAGLIARDI, Pedro. *As liminares em processo penal.* São Paulo: Saraiva, 1999.

GLEITMAN, Henry; FRIDLUND, Alan J.; REISBERG, Daniel. *Psicologia*. 6ª ed. Trad. de Danilo R. Silva. Lisboa: Fundação Calouste Gulbenkian, 2003.

GLEITMAN, Henry; REISBERG, Daniel; GROSS, James. *Psicologia*. 7ª ed. Trad. de Ronaldo Cataldo Costa. Porto Alegre: Artmed, 2009.

HARMON-JONES, Eddie; HARMON-JONES, Cindy. Cognitive dissonance theory after 50 years of development. *Zeitschrift für Sozialpsychologie, 38*(1), 2007, p. 7-16. http://dx.doi.org/10.1024/0044-3514.38.1.7

LOPES JR., Aury; RITTER, Ruiz. A imprescindibilidade do juiz das garantias para uma jurisdição penal imparcial: reflexões a partir da teoria da dissonância cognitiva. *Revista Magister de Direito Penal e Processual Penal.* Porto Alegre, v. 13, n. 73, ago./set. 2016, p. 12-25.

LYNCH, Kevin J. The lock in effect of preliminary injunctions. *Florida Law Review.* Vol. 66, 2014, p. 779-821. Disponível em: <http://www.floridalawreview.com/wp-content/uploads/9-Lynch.pdf>.

MAYA, André Machado. *Imparcialidade e Processo Penal* - Da prevenção da competência ao Juiz de Garantias. Rio de Janeiro: Lumen Juris, 2011.

MYERS, David G. *Psicologia Social.* 10ª ed. Trad. de Daniel Bueno, Maria Cristina Monteiro e Roberto Cataldo Costa. Rio de Janeiro: AMGH Editora, 2014.

PRADO, Lídia Reis de Almeida. Racionalidade e emoção na prestação jurisdicional. In: ZIMERMAN, David; COLTRO, Antônio Carlos Mathias (Orgs.). *Aspectos psicológicos da atividade jurídica*. 3ª ed. Campinas: Millennium, 2002, p. 85-95.

RAMOS, João Gualberto Garcez. *A tutela de urgência no processo penal brasileiro*. Belo Horizonte: Del Rey, 1998.

RITTER, Ruiz. *Imparcialidade no processo penal*: reflexões a partir da teoria da dissonância cognitiva. Florianópolis: Empório do Direito, 2017.

RODRIGUEZ, José Rodrigo. Como decidem as cortes?: para uma crítica do direito (brasileiro). Rio de Janeiro: Editora FGV, 2013.

SILVA, Danielle Souza de Andrade e. *A atuação do juiz no processo penal acusatório*. Incongruências no sistema brasileiro em decorrência do modelo constitucional de 1988. Porto Alegre: Sergio Antonio Fabris, 2005.

SCHÜNEMANN, Bernd. O juiz como um terceiro manipulado no processo penal? Uma confirmação empírica dos efeitos perseverança e correspondência comportamental. *Revista Liberdades*, São Paulo, n. 11, set./dez. 2012, p. 30-50.

TABAK, Benjamin Miranda; AGUIAR, Julio Cesar; NARDI, Ricardo Perin. O viés confirmatório no argumento probatório e sua análise através da inferência para melhor explicação: o afastamento do decisionismo no processo penal. *Revista da Faculdade de Direito da UFMG*. Belo Horizonte, n. 70, jan/jun. 2017, p. 177-196. https://doi.org/10.12818/P.0304-2340.2017v70p177

VIEIRA, Lucas Theodoro Dias, SILVA, Natanael Lud Santos e. O modelo atitudinal de julgamento, os vieses de cognição e a colegialidade corretiva: Breves considerações. In: *Direito na Atualidade*: Uma Análise Multidisciplinar. André Vicente Leite de Freitas, Fernanda Paula Diniz, Henrique Viana Pereira (Organizadores). Rio de Janeiro: Lumen Juris, 2016, p. 83-103.

ZIMERMAN, David. A influência dos fatores psicológicos inconscientes na decisão jurisdicional: a crise do magistrado. In: ZIMERMAN, David; COLTRO, Antônio Carlos Mathias (Orgs.). *Aspectos psicológicos da atividade jurídica*. 3ª ed. Campinas: Millennium, 2002, p. 125-132.

Informações adicionais e declarações dos autores (*integridade científica*)

Agradecimentos (acknowledgement): Agradeço ao Professor Dr. Túlio Lima Vianna, do Programa de Pós-Graduação em Direito (Mestrado e Doutorado) da Faculdade de Direito da Universidade Federal de Minas Gerais, que estimulou o estudo do assunto. Aos amigos Rudson Coutinho da Silva e Eliane Maria de Carvalho, pelo incentivo e troca de ideias. Expresso ainda minha gratidão aos amigos Marco Aurélio Badue Kallas, Maria Helena Soares Ferreira Borges e Guilherme D. P. Sousa, pela gentil colaboração na revisão do texto.

Declaração de conflito de interesses (conflict of interest declaration): o autor confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

Declaração de ineditismo e originalidade (declaration of originality): o autor assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 17/03/2019
- Deslocamento ao V5N3 e aviso ao autor: 17/03/2019
- Controle preliminar e verificação de plágio: 04/07/2019
- Avaliação 1: 11/07/2019
- Avaliação 2: 12/07/2019
- Avaliação 3: 30/07/2019
- Decisão editorial preliminar: 09/09/2019
- Retorno rodada de correções: 30/09/2019
- Decisão editorial final: 08/10/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editor-assistente: 1 (RDG)
- Revisores: 3

COMO CITAR ESTE ARTIGO:

ANDRADE, Flávio da S. A dissonância cognitiva e seus reflexos na tomada da decisão judicial criminal. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1651-1677, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.227

Resenha

Review

Review: Rivera, Iñaki. *Decarceration, principles for a public policy of reduction of the prison reduction (from a radical guarantism)*, Valencia: Tirant lo Blanch, 2017, 252 p.

Resenha: Rivera, Iñaki. Descarcelación, principios para una política pública de reducción de la cárcel (desde un garantismo radical). Valencia: Tirant lo Blanch, 2017, 252 p.

Silvio Cuneo[1]

Universidad Central de Chile

silvio.cuneo@ucentral.cl

http://orcid.org/0000-0003-1072-745X

Following a coherent line of research expounded in a number of various previous publications on prison, Iñaki Rivera, in this latest work presents a realistic and necessary picture of a possible road to mass decarceration. Together with undertaking a comprehensive social and juridical analysis of the complex world of prison and incarceration, the author does not lose sight of the essential aspect, the human being, the unique and exclusive individual who suffers physically and spiritually the brutality of punitive power: he who, from his solitary and silent or overcrowded and noisy cell, feels that his life is not worth living.

The book firmly asserts that the problem of prison must be solved by first seeing to the needs of the inmates themselves, reminding us that *the issue of prison cannot continue to be addressed without its main protagonists, it cannot continue to be examined (only) by "experts"*. However, it recognises

[1] Profesor y Coordinador del Centro de Investigaciones Criminológicas de la Justicia Penal de la Universidad Central de Chil. Doctor en Derecho por la Universitat Pompeu Fabra y la Università degli Studi di Trento. Entre sus libros destacan: "Cárceles y pobreza. Distorsiones del populismo penal" (2018), "El encarcelamiento masivo" (2017), "La cárcel moderna. Una crítica necesaria" (2017) y "Cine y Derecho penal" (2010).

that this problem will hardly be solved inside the prison itself, but rather outside of it, in the same society that creates it, produces it, feeds it and reproduces it. In this light, the best option will never be to "improve" such a savage and violent institution as prison, but to think less and less in terms of prison itself, primarily looking for strategies to contain the influx of new inmates, then its reduction, and finally its radical elimination.

Although it might appear obvious, the book reminds us that not because things stands as they are, they should be like that. Slavery, poverty, social injustice and exploitation, as well as mass and inhuman imprisonment, are not natural phenomena: they are created by society and can and must be changed. Even if something seems unfeasible (for example, the end of discrimination against women or the thousands of daily child deaths from poverty-related causes) this makes it no less morally desirable.

Essentially (although it may not be explicitly acknowledged by the author), it is a juridical-criminal analysis that involves sociological matters and the philosophy of punishment. The author positions his premises of excarceration in a non-static point somewhere between abolitionism and liberal theory of criminal law, leaning towards the latter in order to opt for a possible and necessary path, distancing itself from abolitionist ideals. Rivera's work in this aspect recalls the words of Manuel de Rivacoba who criticised abolition – albeit acknowledging the noble impulses of these aspirations –while reminding us that "unless there is a transmutation in human nature and, consequently, in social demands and institutions, abolition itself is not, as in Stammler's well-known simile, a polar star for sailors, a port to reach and disembark, but it is rather a brilliant idea that is both a guide and a destination which we relentlessly strive to reach, a regulating principle, meaning, a model determining the degree of perfection, that is to say of effectiveness, of different punitive legislation. On the hand, believing it to be attainable and striving to achieve it or accomplish it in our times may well distract our attention and efforts from more urgent and feasible tasks; including fully knowing and rationally applying existing Law, undertaking or continuing a serious and steady process of decriminalisation or advancing along the path of humanisation. Or in other words: what is desirable must not thwart or lead us astray from what is possible; the maximalist aspiration

to the absolute must not frustrate our efforts towards obtaining a truly minimal, sustainable, dignified criminal law".[2]

I would like to stress that this work is a juridical – criminal analysis focusing on the dark and forsaken world of prison conviction. Criminal law, it should be remembered, is a two-faced coin (crimes and punishments, Cesare Beccaria told us just over 250 years ago). However, it seems that criminal lawyers have forgotten about punishment, and in their manuals, treaties, monographs, etc. they dedicate themselves almost exclusively to the analysis of the theory of crime, more and more abstractly, from up high, omitting almost any kind of reference to the world of punishment. Several professors of criminal law fail to lower themselves to the reality of the sentence, ignorant of prisons, and their silence ends up legitimising this space which is a legislative void or a negation of Rights. In this way, prison expands without losing its aspect of a space devoid of justice, forgotten by the criminal lawyers. This book, on the contrary, invites us to enter the world of prison, and perhaps even more importantly, it calls for the opening up of prison, so that prison itself becomes less prison (quantitatively and qualitatively) and is understood as part of a society that must respect the human rights of all people, whether they be free or imprisoned.

Iñaki Rivera's book does not lose sight, like the polar star, of the concept of the individual. It also reminds us that since the International Human Rights Law, there has been a globally recognized idea of the individual, established in international covenants – concerning penal issues, criminal procedure and prison, and especially in the Universal Declaration of Human Rights which places limits on state interference or behaviour and compels us not to exploit our fellow humans. These agreements integrate the legal systems, within which they are made a priority. As such, legislation, regulations and official practices must therefore be brought in line with them. All of the legal system must be consistent with itself, logically and axiologically. A conception of prison is also to have a conception of the penalty and a conception of the penalty is to have that of the human being.

---

[2] RIVACOBA, Manuel de, *Función y aplicación de la pena*, Depalma, Buenos Aires, 1993, p. XII

Rivera exposes the fallacies of arguments legitimising prison, particularly the positivity of prevention fallacy (the rhetoric of rehabilitation) based on the idea that it is possible to teach people to live in freedom by depriving convicts of their freedom. Likewise, the book harshly criticises authoritarian conceptions of criminal law by eminent personages that, rather than prosecute specific deeds, punish personalities and ways of being, labelling convicts and ascribing them future behaviour based on the illusion of being able to foresee risks. On the other hand the book also is strongly critical of penetrating conceptions that contain and foment a declared hostility towards he who is increasingly seen as the "other", someone different who can acquire monstrous morphologies (terrorist, paedophile or serial killer), but who is usually an *ugly, dirty and bad* common criminal (paraphrasing a film by Ettore Scola). Alarmist concepts encourage the control and confinement of enemies, convincing us that *our* security depends on *their* control.

Rivera reminds us according to this conception, politics assumes the characteristic feature of conflict since any divergence of interests can at some point be transformed into rivalry or antagonism between people or social groups. Such arguments obtain enormous electoral consensus for politicians who promise the massive confinement of enemies of public order. To legitimise these bellicose, antiliberal and antidemocratic policies, pseudo criminologists appear who, with scientific semblance, echo social demands (previously inflamed by disproportionate fear), and opinionists, masquerading as specialists, set up centres of "study" flanking political spheres that hold power (for example, the Manhattan Institute in the United States, the *Fundación Paz Ciudadana* in Chile, etc.) creating a distorted image of criminality where the common criminal (read poor and marginal) is an enemy undeserving of any rights, who must be imprisoned.

Rivera also looks with distrust at the so-called alternative forms to prison, since these exist alongside prison. For these, prison still maintains a central role and the so-called alternatives are in need of prison in order to operate. In the same way, experience teaches us - or should teach us - that the implementation of alternative sentences to prison often does not translate in a reduction in prison sentences, but only in an expansion of the punitive network.

As for the actual carrying out of the custodial sentence, Rivera denounces *prison within the prison,* an implementation that does not respect the principle of legality (nor those of proportionality, guilt, offensiveness, certainty, concreteness and humanity), operating with a high discretionary power based on the assessment of the personality of the detainee. It is, in Ferrajoli's words, a substantially arbitrary and anti-liberal power that contradicts the founding principle of guaranteeing the criminal's rights according to which you cannot be punished for *what you are*, but for *what you have done*.

After analysing the multi and devastating effects prison produces on those who experience it, Riviera, on citing Gonin and Pavarini, confines prison's history in the broader history of hypocrisy. Prison is no more humane than the atrocious public penalties that went before it in history. The main difference has not so much to do with the respect or the dignity of the prisoner as it has with the sensitivity of a society that preferred not to witness human suffering. Thus, prison conceals suffering within four walls. Therefore, the pain of convicts, although known, can be ignored. We are all aware of what occurs inside prison and we seem to accept it without further questioning; however, at the same time we deny the fact. We cannot conceive that our prisons are only for the poor and that they constitute only a system of oppression for people to whom we have denied education, health and housing.

Stanley Cohen coined the concept of *a state of denial*, according to which people are familiar and are not familiar at the same time with a certain phenomenon. Today we know and we do not know that prison is an inhuman space. We know that every year a high number of poor people will be imprisoned, and we know as well that they could die, be injured, be raped by other inmates or tortured by police officers. However, since we know that prisoners are from slums and that they behave in a way exactly opposite to us, we do not care. Somehow, we believe that they deserve what they are experiencing or that they are predestined to it, but if we question what they deserve in relation to what we have given them and what we demand of them, we know (or we do not know) that they do not deserve all the injustices they are forced to live (hunger, lack of opportunities, lack of decent housing and basic necessities, impossibility to go to university, high probability of ending up in prison, etc.). Prison

is inhuman; however, the denial of prison's reality is easy because we know that we will never have to suffer it.

Iñaki Rivera, who is familiar with the forces that maintain and promote prison, is well aware that the outlook is adverse and, despite the pessimism - that in this subject is also realism -, is not discouraged and shows us a possible and necessary way to contain mass imprisonment and thus take human rights seriously.

The book, I highlight, points out the existence of a possible and unavoidable path. It illustrates more than a hundred proposals, recommendations and alternatives for a public policy whose goal is decarceration. These are feasible proposals that seem to be the only possible way to respect international human rights law. This position of "radical guarantee" invites us to seriously take the fundamental rights of people deprived of their liberty and, on that basis, to define a programme of constant decarceration. Such proposal does not only mean respect for the human rights of prisoners, since by dehumanising such a person we also dehumanise ourselves, and massive dehumanisation necessarily means the dehumanisation of society. And this is just so, even if we are not aware of the pain of prisoners. Mass imprisonment, like a silent ghost, corrodes the freedom of all and ends up taking away the most precious thing of life itself.

On the other hand, the criminal effects that prison produces will be a price to be paid in the future and will translate into more crimes and higher levels of violence, which will also generate more prisons, more controls, more police and, in addition, more prisoners. In this way, mass incarceration, like an upward spiral, has as its point of arrival the confinement of all. Only a change of direction, a shift towards respect for human dignity, can help us avoid a suicidal policy.

Informações adicionais e declarações dos autores (*integridade científica*)

Declaração de conflito de interesses (conflict of interest declaration): o autor confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação desta resenha.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria desta resenha estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

Declaração de ineditismo e originalidade (declaration of originality): o autor assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 22/01/2019
- Controle preliminar e verificação de plágio: 29/01/2019
- Deslocamento ao V5N2: 17/02/2019
- Decisão editorial preliminar e deslocamento ao V5N3: 23/05/2019
- Retorno rodada de correções: 29/09/2019
- Decisão editorial final: 30/09/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editor-associado: 1 (BC)

COMO CITAR ESTE ARTIGO:

CUNEO, Silvio. Review: Rivera, Iñaki. Decarceration, principles for a public policy of reduction of the prison reduction (from a radical guarantism). *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1681-1688, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.282