Regina Linden Ruaro
José Luis Piñar Mañas
Carlos Alberto Molinaro
(Orgs.)

Privacidade e Proteção de Dados Pessoais na Sociedade Digital

37

Muitas de nossas atividades deixam um rastro de dados. Isso inclui desde registros de telefone, transações de cartão de crédito, GPS em carros que rastreiam nossas posições, telefones celulares (com ou sem GPS) e a lista está crescendo. Um dado pessoal isolado não representa problema mas quando agregado a outros, estabelece-se trilha de informações que os provedores de serviços coletarão, como mensagens instantâneas, navegando em sites ou assistindo vídeos. Essa coletânea que trata da privacidade e dados pessoais é arrecadada, armazenada e pode ser compartilhada com outros - sem o seu consentimento! Por que a privacidade é importante? A privacidade é a capacidade de controlar quem pode acessar informações sobre nossa vida privada e nossas atividades. A privacidade nos dá o poder de escolher nossos pensamentos e sentimentos e com quem os compartilhamos. A privacidade protege s informações que não queremos compartilhar publicamente (como saúde ou finanças pessoais). A privacidade ajuda a proteger nossa segurança física. A privacidade ajuda a nos proteger como indivíduos e nossos negócios, contra entidades de que dependemos ou que são mais poderosas do que nós. A privacidade está ligada à liberdade. Poderíamos realmente ser livres sem privacidade? Felizmente, a privacidade não está morta (ainda), mas está sob ameaça. Sem privacidade, nos tornaremos facilmente controlados, manipulados e com perda de controle sobre nós mesmos e sobre nossas vidas pessoais. Nesse contexto, esta obra coletiva se destina a enfrentar questões e tensões oriundas dessa nova realidade tecnológica. Aproveitemos a sua leitura.

9 788556 961938

editora fi
www.editorafi.org

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DIGITAL

Série
Ciências Jurídicas & Sociais

Comitê editorial da

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DIGITAL

Regina Linden Ruaro
José Luis Piñar Mañas
Carlos Alberto Molinaro
(Orgs.)

φ editora fi

Direção editorial: Liane Tabarelli
Marcia Andrea Bühring
Orci Paulino Bretanha Teixeira
Voltaire de Lima Moraes

Diagramação e capa: Lucas Fontella Margoni

Arte de capa: Internet

O padrão ortográfico, o sistema de citações e referências bibliográficas são prerrogativas do autor. Da mesma forma, o conteúdo da obra é de inteira e exclusiva responsabilidade de seu autor.

http://www.abecbrasil.org.br

Série Ciências Jurídicas & Sociais - 37

Dados Internacionais de Catalogação na Publicação (CIP)

RUARO, Regina Linden; MAÑAS, José Luis Piñar, Molinaro, Carlos Alberto (Orgs.)..

Privacidade e proteção de dados pessoais na sociedade digital. [recurso eletrônico] / Regina Linden Ruaro; José Luis Piñar Mañas; Carlos Alberto Molinaro (Orgs.) -- Porto Alegre, RS: Editora Fi, 2017.

192 p.

ISBN - 978-85-5696-193-8

Disponível em: http://www.editorafi.org

1. Direito penal. 2. Privacidade. 3. Sociedade. 4. Dados pessoais. I. Título. II. Série

CDD-340

Índices para catálogo sistemático:
1. Direito 340

SUMÁRIO

APRESENTAÇÃO 9

CONFLITO REAL OU APARENTE DE INTERESSES ENTRE O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E O LIVRE MERCADO
Regina Linden Ruaro; Carlos Alberto Molinaro 13

A TROCA INTERNACIONAL DE INFORMAÇÕES FISCAIS E OS DIREITOS DO CONTRIBUINTE
Paulo Caliendo 47

DERECHO, TECNICA E INNOVACIÓN EN LAS LLAMADAS CIUDADES INTELIGENTES. PRIVACIDAD Y GOBIERNO ABIERTO
José Luis Piñar Mañas 59

REFLEXÕES PÓS-PANÓPTICAS SOBRE VIGILÂNCIA E CONSUMO NA SOCIEDADE DA CLASSIFICAÇÃO
Andrea Cristina Versuti; Marco Aurélio Rodrigues da Cunha e Cruz 83

COOPERAÇÃO ENTRE ESTADOS TOTALITÁRIOS E CORPORAÇÕES: O USO DA SEGMENTAÇÃO DE DADOS E PROFILING PARA VIOLAÇÃO DE DIREITOS HUMANOS
Cinthia Obladen de Almendra Freitas; Danielle Anne Pamplona 119

MUTAÇÕES DA PRIVACIDADE E A PROTEÇÃO DOS DADOS PESSOAIS
Têmis Limberger 145

LAS CONSECUENCIAS DEL BREXIT SOBRE EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES
Alejandro Corral Sastre 169

APRESENTAÇÃO

Nos encontramos, permanentemente, em processo de avanços tecnológicos e estes, por óbvio, não podem ser atribuídos a fatos e períodos específicos ou momentâneos porque importam em aquisição de conhecimento. É que conhecimento se produz através dos tempos e a partir de pesquisas científicas que mais e mais se aprofundam, remodelam e se aperfeiçoam. A par disto, para chegar-se ao uso das novas tecnologias de comunicação e informação, impõe-se rememorar, sobretudo, grandes inventos como a imprensa escrita, o telefone e o telégrafo considerados de um importante papel na comunicação. A este último pode-se agregar, ainda, o fato de que se prestava para troca de informações registradas e muitas vezes de caráter privado e contendo dados pessoais.

Seguindo-se no tempo, um importante passo no uso das atuais TIC, como mecanismo de recolhimento, catalogação e tratamento de dados temos a criação, por Herman Hollerith, em 1884, dos cartões perfurados destinados ao tratamento com automação de informações e dados pessoais. Hollerith fundou, em 1896, a empresa Tabulating Machine Company que foi a precursora da International Business Corporation (IBM).

A metodologia empregada com a tabulação de dados pela empresa de Hollerith possibilitou uma redução de dois anos e meio no censo de 1890 nos Estados Unidos relativamente ao censo anterior realizado em 1880. Mais do que isto, os cartões perfurados permitiam classificar as pessoas de determinada localidade de forma a saber quantas eram do sexo feminino ou masculino, raça, estado civil, idade. O avanço foi de grande valia, por outro lado, permitiu que os nazistas utilizassem o sistema de Hollerith para catalogar as pessoas que se encontravam nos campos de concentração atribuindo-lhes códigos em números o que lhes permitia saber quem era homossexual, antissocial, cigano e judeu propiciando assim o genocídio perpetrado por Hitller.

Sem sombra de dúvidas, os avanços aportados pelas TIC a partir dos anos sessenta com o uso dos modernos computadores, rapidamente se espalhou pelo mundo em todos os espaços. No entanto, para as primeiras máquinas, “interatividade” ainda era uma palavra distante. O tão conhecido processamento de dados, gradativamente, debruçou-se

sobre as técnicas aplicadas a esta tecnologia cada vez mais aperfeiçoando-a.

Houve época em que um computador era tido pela população como uma máquina colossal, de difícil manejo e assimilação, posteriormente, passou-se a uma nova etapa do fenômeno tecnológico resultante da introdução dos "computadores pessoais" no mercado, entre os anos 80 e 90, estes libertaram a informática dos centros especializados, das universidades e das grandes empresas.

Com o advento do computador pessoal, possibilitou-se o armazenamento e avaliação de dados relativos à vida dos indivíduos sem a necessidade de existência de um complexo programa apropriado para tal propósito. Alguns setores sociais perceberam nisso quão útil poderia ser coletar, tratar e armazenar, para posterior uso ou transferência ou divulgação, os dados pessoais a terceiros.

O surgimento da Internet incrementou ainda mais a capacidade de comunicação, de tal forma que a sociedade passou a ter uma nova organização, na qual a posse de dados e informações transformou-se em poder onde aqueles se constituem na matéria prima para o novo formato de capitalismo que se instala na nossa sociedade a qual passou-se a denominar de sociedade digital.

Não resta dúvidas de que esses incrementos tecnológicos proporcionam inúmeras facilidades, dentre as quais se destaca a velocidade e a praticidade de acesso à informação, em especial por meio dos buscadores simples como o Google, Bing, Ask, Yahoo, dentre outros e a vantagem do imediatismo e da economia dos meios de comunicação instantânea e "gratuita", como por exemplo, Watzzap, Skipe, Facebook, Messenger, Telegram, Twiter.

O que mais chama a atenção é que com popularização dessas ferramentas, o que antes era somente uma facilidade torna-se hoje uma necessidade para o desenvolvimento social e econômico, é que os avanços tecnológicos na comunicação e informação não estão limitadas por barreiras espaciais ou temporais, em consequência, incorporam um risco implícito de exposição pessoal que ultrapassa barreiras e estende-se a nível mundial, sua utilização deixa rastros permitindo que terceiros obtenham (in)discriminadamente dados e informações. Este fato que aparentemente só traz vantagens, pode, no entanto, produzir afronta a

direitos fundamentais como a intimidade, privacidade e uso indiscriminado de dos dados pessoais.

Tal cenário demonstra a complexidade da tarefa do Direito e dos legisladores em enfrentar os desafios na busca de compatibilizar os direitos fundamentais abrangidos com os avanços das TIC que mais e mais tornam esta tarefa árdua e difícil face ao gritante descompasso existente entre ambos.

Derradeiramente, no momento ao qual nos encontramos, a proteção jurídica dos direitos fundamentais à privacidade e à proteção de dados pessoais requer uma especial atenção da ordem jurídica que leve em conta novos modelos que se adaptem a esta incerta realidade. Mais que nada há a necessidade de compreender que não se pode engessar as TIC seja porque seria plantar em terreno árido, ou tentar "colocar portas no campo"; seja porque o Direito tem de adaptar-se neste contexto dando uma resposta à frente de seu tempo.

Efetivamente, este livro não pretende esgotar o tema e nem poderia. A matéria está em ebulição no mundo todo, o Brasil, por sua vez, enfrenta um descompasso por não contar com legislação específica em matéria proteção de dados pessoais, ao contrário, da União Europeia vem constantemente aperfeiçoando suas normativas a fim de adaptá-las à nova realidade tecnológica e aos interesses de ordem social e econômica. Por tal motivo, em face desta lacuna em nosso ordenamento jurídico, direitos fundamentais padecem muitas vezes de tutela efetiva e geram prejuízos pessoais, sociais e econômicos para a nação.

Nesse contexto, a obra coletiva se destina a enfrentar questões e tensões oriundas da nova realidade tecnológica. Este livro é resultado de projetos de pesquisa conjunta realizada no Programa de Pós-Graduação em Direito da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS através de Grupos de pesquisa e de sua Coordenação. A pesquisa foi parcialmente financiada pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico- CNPq - Editais Universal 14/2008 e 14/2013, em conjunto com a Universidad San Pablo-CEU de Madri/Espanha no Projeto de Pesquisa sobre Protección de Datos, Seguridad e Innovación: Retos en un mundo global tras el Reglamento Europeo de Protección de Datos, Ref. DER2016-79819-R, do Programa I+D do Ministério de Economia e Competitividade desse país.

Ao longo de todo o projeto se realizaram seminários no Brasil e na Espanha, foram proferidas palestras no Master em Protección de Datos Personales da Universidade San Pablo-CEU de Madri, bem como, a realização de estágio docência pela Profa. Dra. Regina Linden Ruaro uma das organizadoras da obra e que faz parte do Grupo internacional de pesquisa liderado pelo Prof. José Luis Piñar Mañas e Coordenador do Projeto internacional (www.privacidadyacceso.es).

Integram a obra professores brasileiros e espanhóis, pesquisadores na área objeto deste livro e que foram convidados a fim de enriquecer o trabalho com as suas pesquisas. Assim, tivemos a honra de contar com: Profa. Dra. Andrea Cristina Versuti, do PPGE da Universidade de Brasília; Profa. Dra. Cíntia Obladen de Almeida Freitas, do PPGD em Direito da PUCPR; Profa. Dra. Danielle Anne Pamplona, do PPGD da PUCPR; Prof. Dr. Marco Aurélio Rodrigues da Cunha e Cruz, do PPGD da UNIOESC; Profa. Dra. Têmis Limberger, do PPGD da UNISINOS;; Prof. Dr. Paulo Caliendo, do PPGD da PUCRS; e Prof. Dr. Alejandro Corral Sastre, do PPGD Universidade San Pablo - CEU de Madri/Espanha.

Por fim, cabe agradecer, primeiramente, o apoio e incentivo recebido do Coordenador do PPG em Direito da PUCRS, Prof. Ingo Sarlet que tem, incansavelmente, investido na capacitação dos docentes e discentes do PPGD e que foi responsável pelo estabelecimento da Rede de interação entre os Programas que participam da obra, também, agradecer o fomento recebido pelo CNPq e pelo Ministério de Economia e Competitividade da Espanha, a Universidade San Pablo CEU de Madri que abriu suas portas para que professores, mestrandos e doutorandos do PPGD da PUCRS pudessem agregar pesquisas aos seus trabalhos, bem como, a todos os professores colaboradores que enviaram seus textos e que só enobrecem e valorizam a obra coletiva.

Porto Alegre e Madri, setembro de 2017.

Regina Linden Ruaro
Carlos Alberto Molinaro
José Luis Piñar Mañas

CONFLITO REAL OU APARENTE DE INTERESSES ENTRE O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E O LIVRE MERCADO

Regina Linden Ruaro[1]
Carlos Alberto Molinaro[2]

Introdução

O direito à privacidade, que na Constituição Federal brasileira está previsto como um direito à vida privada busca proteger o indivíduo de invasões de terceiros na sua esfera pessoal e à proteção de dados pessoais. No entanto, com o avanço das tecnologias e o alto processamento de informações pessoais modificou-se o sentido e o espectro desses meios "clássicos" de violações. Tal realidade acabou acarretando um novo perfil e uma (re)significação do que hoje entendemos por privacidade[3]. É que há, duas concepções importantes para compreensão de onde parte a proteção dos dados pessoais. Neste sentido, tem-se a *privacy* americana que incorpora aquele aproximando-o do direito à intimidade e, de outro modo, o sistema da UE que o tem como um direito fundamental autônomo como se verá no decorrer deste artigo.

Independentemente disso e para qualquer um dos sistemas, os dados pessoais têm um grande valor, tanto para o setor público, quanto para o privado é que através deles é possível formar perfis sobre comportamento, consumo e até mesmo sobre características genéticas. Além disso, cada vez mais, são elementos essenciais para as que as pessoas consigam estabelecer relações dentro da sociedade.

---

[1] Professora Titular da Pontifícia Universidade do Rio Grande do Sul – PUCRS. Doutora em Direito pela Universidad Complutense de Madrid (1993) com Pós-doutorado na Universidad de San Pablo-CEU de Madrid (2008). Membro do Grupo Internacional de Pesquisa em Proteção de Dados Pessoais – Privacidad y Acceso – www.privacidadyacceso.es. E-mail: ruaro@pucrs.br.

[2] Professor do Programa de Pós-Graduação em Direito (Mestrado e Doutorado) da Pontifícia Universidade Católica do Rio Grande do Sul. Doutor em Direito.

[3] DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006.

O presente ensaio busca discutir e refletir acerca dos conflitos (reais e/ou aparentes) de interesses resultantes do direito fundamental à privacidade, à proteção de dados pessoais e o comércio de banco de dados. Com o objetivo de estudar este tema, mas sem pretender esgotar a matéria, far-se-á, preliminarmente, uma análise dos principais sistemas jurídicos que abordam o direito à privacidade e a proteção de dados pessoais[4], tendo como base o sistema americano e o europeu, facilitando assim a melhor compreensão do fenômeno que representa, nas palavras de Danilo Doneda, uma pretensa "afirmação do direito como estrutura [...] para que as escolhas relativas às questões que agora enfrentamos sejam realizadas mediante o respeito de valores fundamentais do ordenamento".[5]

Em consequência dessa realidade temos que, por ser o dado pessoal uma informação, quem a detém tem poder, o que acaba atribuir-lhe um valor econômico a ser comercializado em determinadas circunstâncias. Tal realidade, no Brasil, vai se tornando palpável e bem demonstra a Decisão do Tribunal de Justiça do Rio Grande do Sul na Apelação Cível 70069420503 do ano de 2016 pela qual, ao julgar, a Ação Coletiva interposta pelo Ministério Público contra a Confederação Nacional de Dirigentes Lojistas – SPC BRASIL entendeu que é perfeitamente legal e constitucional a comercialização de bancos de dados pessoais, sem prévio consentimento do sujeito titular dos dados para fins de prospecção de clientes. Escolheu-se esse julgado tendo em vista sua atualidade e o fato de que o mesmo reflete a tensão entre os direitos fundamentais, princípios e mercado, bem como tece uma interpretação que tem consequências na dignidade da pessoa humana.

Para tanto se utilizou como metodologia o método de interpretação jurídica pautado na coleta e análise de bibliografia, legislações e a jurisprudência na matéria. Salienta-se, que o presente artigo está ancorado na linha de pesquisa "Direito, Ciência, Tecnologia & Inovação" no Projetos de Pesquisa, "A proteção dos dados pessoais na sociedade de vigilância: o direito fundamental a privacidade" do

---

[4] Por questões de adaptação á terminologia utilizada na Lei de acesso à Informação (12.527/2011) esclarece-se que dado pessoal entende-se como sinônimo de informação pessoal no presente trabalho.

[5] DONEDA. **Da privacidade à proteção de dados pessoais**. 2006, p. 407.

Programa de Pós-Graduação em Direito da PUCRS, com fomento do CNPq através de Editais Universal dos anos de 2008 e 2013, bem como, dentro de um Projeto maior, internacional, capitaneado pela Universidad San Pablo - CEU de Madrid/Espanha financiado pelo Ministério de Economia y Competitividad daquele país. Referência DER 2009-13.184.[6]

1. Sistema de proteção de dados pessoais nos Estados Unidos – *Privacy* -como referência na compreensão da privacidade

O direito à privacidade tem suas origens no direito norte-americano. No século XX, a população dos Estados Unidos era basicamente rural, sendo a propriedade o principal enfoque das contendas judiciais. A partir da Revolução Industrial, as pessoas começaram a migrar para as cidades paralelamente, as vias de notícias e informações têm um progresso substancial. Diante dessa realidade, começa-se a realizar discussões acadêmicas sobre a proteção da intimidade e da privacidade. A proteção de dados no sistema jurídico américa deriva da chamada *privac*y, não se constituindo de um direito autônomo.

Os dois grandes personagens responsáveis pela discussão desse tema foram Samuel Warren e Louis Brandeis. No artigo The Right to the privacy, publicado na Revista de Direito de Univerdade de Harvad do ano de 1890[7]. Os estudiosos destacaram o desenvolvimento do mercado de notícias e informações, principalmente aquelas de conotações invasivas, o que isso feria um direito básico à proteção da intimidade (uma propriedade intangível) das pessoas. Além disso, os autores também defenderam o "direito de estar sozinho" (antigo paradigma de *zero-relationship*).

O ponto relevante do estudo dos juristas está em que foi Warren quem, pela primeira vez nos Estados Unidos, mostrou-se receoso diante da ampla liberdade da imprensa e seu potencial lesivo, fundado

---

[6] www.privacidadyacceso.es

[7] WARREN, Samuel D. BRANDES, Louis D. The Right to Privacy.**In: Harvard Law Review**, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220. Disponível em: <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>. Acesso em: Março de 2017.

em sua própria experiência pessoal, já que sua vida era constantemente devassada pelos jornais, motivando-o, com o auxílio de Brandeis, a verificar se no sistema norte-americano de C*ommon Law* havia alguma defesa contra as intromissões perpetradas pela imprensa[8]. Os autores realizaram uma análise de precedentes da Corte norte-americana, extraindo desses um direito geral à privacidade, que partia dos clássicos direitos de liberdade e propriedade. O ponto de partida do artigo consistia na formulação da privacidade com base na conjunção de *privacy-property*, segundo a qual a violação ocorria nos casos em que um estranho intervinha no círculo privado de outrem, ou seja, quando houvesse efetiva intromissão física. Posteriormente, os autores vincularam a privacidade a uma noção de liberdade, perpassando pela inviolabilidade da personalidade humana[9].

Em razão de seus estudos os mesmos são os responsáveis pela alteração dos fundamentos jurídicos de defesa dos direitos da personalidade – em específico o *right to privacy* –, visto que, a partir de seu intento, houve a migração das bases jurídicas de defesa de tais direitos do ideal de propriedade para o da dignidade do homem e da inviolabilidade da personalidade humana, ou seja, um direito de natureza aberta e fundamental[10]. No que toca a sistemática jurídica dos EUA, o artigo serviu como base para toda uma nova forma de pensar a privacidade, assim como referência intelectiva para que esta atingisse o patamar de direito constitucionalmente reconhecido[11].

Tendo observado que o surgimento de novas técnicas no campo da fotografia – possibilidade de fotografias instantâneas – viabilizaram a invasão da vida privada dos indivíduos, buscaram identificar a existência de algum elemento de defesa oponível a este

---

[8] MARTÍNEZ, Ricardo Martínez. **Una aproximación crítica a la autodeterminación informativa**. Madrid: Thomson Civitas, 2004. p. 66-67.

[9] LIMBERGER, **O direito à intimidade na era da informática:** a necessidade de proteção de dados pessoais. Porto Alegre: Livraria do Advogado, 2007, p. 55-57.

[10] Nas palavras do autor: [...] Su gran mérito, aparte de definir con clarividencia los elementos esenciales del derecho reside en haber lo concebido como un derecho de textura abierta y naturaleza fundamental al trasladar su fundamento desde el paradigma del derecho de propriedad a La inviolabilidad y dignidad del se humana, al ámbito del derecho de la personalidad. [...] (MARTÍNEZ, 2004, p. 68.).

[11] DONEDA, 2006, p.139.

noviço fato social. Para tanto, partiram da construção do Juiz Thomas Cooley que, em 1888, na obra *A Treatise on the Law of Tort sor the Wrongs Which Arise Independent of Contract*,[12] já havia mencionado a existência de um *right to be let alone*[13]. Nessa conjuntura, o ponto fulcral do estudo estava vinculado à verificação da existência de um direito à privacidade na jurisprudência norte-americana e como se dava sua tutela, qual era sua natureza e seu alcance. Dentre as conclusões dos estudiosos, destaca-se a de que a tradicional garantia prestada à privacidade – estritamente apensada ao direito de propriedade -, não mais se fazia suficiente. Na concepção dos juristas, a privacidade deveria ser analisada a partir de um novo paradigma, afastado das premissas do direito de propriedade e para além da questão da veracidade ou não das informações publicadas pela imprensa a respeito de determinado indivíduo, migrando para o paradigma integridade da pessoa sobre a qual a informação dizia respeito[14]. Nesse sentido, fizeram uso da premissa de que os direitos não podem ser vistos como estáticos ou imutáveis, devendo ser entendidos a partir da realidade que os cerca. Desse modo, analisaram diferentes direitos e suas respectivas transformações no tempo em face da realidade social.[15]

Do exame atento da jurisprudência norte-americana - considerando, por certo, o período histórico - esses juristas notaram que o direito à propriedade era capaz de proteger manuscritos e obras de arte, essencialmente por conta da sua natureza. No entanto, o mesmo

---

12 Cooley, Thomas M. A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract. Chicago: Callaghan, 1879. Uma cópia deste livro pode ser obtida em online em <http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1010&context=books> link permanente.

13 WARREN; BRANDEIS, 1890, p. 193 e ss.

14 WARREN; BRANDEIS, 1890.

15 A presente transcrição elucida o exposto: [...] Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, -- the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession - intangible, as well as tangible [...] (WARREN; BRANDEIS, 1890, p. 193).

não era suficiente quando o ponto em questão fossem bens imateriais, tais como a paz de espírito e a possibilidade de proibição de publicação de fatos ou informações indesejadas que dissessem respeito tão somente à própria pessoa.[16] De fato, até então, a jurisprudência americana decidia tais demandas com base nos direitos de propriedade. Porém, os doutrinadores perceberam a necessidade de sustentar um direito vinculado à própria pessoa, a qual serviu como sustentáculo para o desenvolvimento de uma matriz argumentativa alienada dos ditames do direito de propriedade, calcada nos direitos de personalidade e na própria dignidade da pessoa humana. Nesse passo, entenderam que se a ficção da propriedade, em sentido estrito, deveria ser preservada, ainda seria verdade que o fim atingido pelo fomentador das especulações da vida alheia seria obtido através daquilo que não lhe pertencia, ou seja, dos fatos cujo titular considerou apropriado manter sob proteção da sua esfera privada. Nesse aspecto, trouxeram citação proferida pelo Lorde Cottenham, em 1820, em uma nota manuscrita acerca do caso Wyatt v. Wilson, onde constou que o homem tem o direito de ser protegido naquilo que é exclusivamente seu.[17] Tais considerações levaram os juristas a crerem que a proteção conferida aos pensamentos, sentimentos e emoções, por meio da escrita ou das artes, não visava nada mais do que impedir a exposição individual, sendo uma instância do direito mais geral do indivíduo de ser deixado em paz, anteriormente recitada pelo Juiz Cooley. Logo, o que estaria a se proteger não era o princípio da propriedade privada, mas, sim, a inviolabilidade pessoal.[18] A partir disto, verificaram a existência de um direito que poderia ser invocado para a proteção da privacidade do indivíduo contra a invasão da imprensa, do fotógrafo ou do dono de qualquer moderno dispositivo capaz de gravar

---

16 WARREN; BRANDEIS, 1890.

17 WARREN; BRANDEIS, 1890.

18 "[...] These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. [...]The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality." (WARREN; BRANDEIS, 1890, p. 205).

ou reproduzir cenas ou sons. Logo, aduziram que se há proteção às emoções e sensações expostas em uma obra musical, igual proteção haveria dos pensamentos e emoções expressos na forma escrita, em comportamentos, conversas, atitudes ou expressões faciais[19]

No sistema americano a concepção de "privacy" se compõe do direito à privacidade e da proteção de informações pessoais e pode-se verificar, a partir dos estudos de John L. Mills[20], que elenca quatro esferas da privacidade, sendo que dentre elas está a proteção pessoal da informação ao qual chamou de "The Personal-Information Sphere: Protecting Personal Data". Nesta esfera, se está diante da proteção de dados pessoais enquanto derivada da privacidade. Trata-se do controle da informação pessoal, que é a esfera menos desenvolvida e protegida no direito americano. Nesta concepção, as pessoas procuram proteger suas informações, ou não as tornando públicas, ou tentando reparar os danos causados pela sua publicação indevida. Nesse sentido a Suprema Corte dos Estados Unidos concluiu que privacidade constitucional inclui não somente "interesse na independência para se tomar certos tipos de decisões importantes" como também "interesse individual em evitar a abertura de interesses pessoais." Ainda assim, informações pessoais são minimamente protegidas neste sistema.

As informações pessoais podem ser protegidas também pelos princípios do direito civil americano tais como: "*false light, defamation, public disclosure of facts e intrusion upon seclusion*", todos baseados em uma "expectativa razoável" de privacidade contra cada intrusão. Existem varias formas de informação pessoal, algumas muito íntimas, que

---

[19] Os juristas abordaram, ainda, as causas de decidir apresentadas pelos tribunais nos casos Prince Albert v. Strange (1849) e Tuck v. Priestes (1887), no qual a defesa do righttoprivacy não se deu com base no direito à propriedade, porém com fulcro na quebra da confiança. Muito embora isso, conferiram que os tribunais notaram que tal justificativa não seria apta em certos casos, a título de exemplo citaram o envio de correspondência, onde em um primeiro momento remetente e destinatário não possuem qualquer pacto entre si. Logo, em razão da insuficiência do argumento decisório, retornaram os tribunais ao fundamento albergado no direito à propriedade (WARREN; BRANDEIS, 1890).

[20] *Privacy:* the lost right. New York: Oxford University Press, 2008.

RABELO, Iglesias Fernanda de Azevedo e GARCIA, Filipe Rodrigues. **O direito à autodeterminação informativa**. Disponível em <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10473> Acesso em: 07 out 2014.

só serão conhecidas se a pessoa quiser compartilhá-las, e outras, também íntimas, mas que são compartilhadas com médicos, padres e advogados. Para a obtenção de algumas são necessárias para licenças, como por exemplo, em viagens e alguns tipos de compras, mas mesmo sendo dadas de forma voluntária, não se permite que sejam tornadas públicas sem qualquer controle.

O nível de controle das pessoas sobre suas informações acabará gerando conflitos de segurança e de interesse comercial. A proteção dessa esfera se dá por Constituições dos Estados ou *tort law*, como *defamation, false light, public disclosure of private facts*. Não obstante a isto, com as crescentes transformações na forma de interagir da sociedade, em especial diante das TIC - Tecnologias da Informação e Comunicação, esta concepção foi, progressivamente, se tornando insuficiente para contemplar todos os aspectos da privacidade. Como bem aponta Stefano Rodotà[21], o direito à privacidade, hoje, não importa somente na faculdade de termos nossa vida privada preservada, mas também na possibilidade de controlarmos a disponibilização de nossos dados[22].

É justamente neste ponto que se verifica a intersecção do direito à privacidade com o direito à proteção de dados pessoais e que diferencia-se da concepção europeia porquanto esta última separa ambos os direitos.

2. A construção de um direito fundamental à proteção de dados pessoais na UE: a autodeterminação informativa

Na Carta dos Direitos Fundamentais da União Europeia é assegurado o direito à vida privada e o direito à proteção dos dados

---

21 RODOTÁ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

22 Frente aos novos desafios, é cada vez mais claro que o sentido de isolamento predominante na doutrina do direito à privacidade do tempo de Brandeis e Warren está superado. Neste novo panorama, a privacidade deixa de ser um meio de garantir o isolamento de alguns para cumprir também uma outra função, que é reagir contra políticas de discriminação baseadas em opiniões e opções religiosas, políticas e sexuais, bem como de toda sorte de informações privadas (RODOTÀ, 2008, p. 117).

pessoais. O artigo oitavo da referida Carta[23] elenca uma série de comandos que devem ser observados para a efetiva proteção dos dados pessoais. São eles: tratamento leal; fins específicos; existência de consentimento; fundamento legítimo previsto em lei; ter direito de aceder, isto é, ter direito de acesso e; ter direito de ratificação. Ademais, a Carta também fala de uma autoridade que fiscalize a efetivação dos direitos citados.

Além das garantias asseguradas pela Carta dos Direitos Fundamentais, foi promulgada Diretiva 46/95/CE que trata sobre o tratamento de dados pessoais e a livre circulação dos dados.

Na Alemanha existe a Lei de Proteção contra o emprego abusivo de dados de identificação pessoal no âmbito do tratamento de dados. Uma de suas principais características é a proibição de consultar, modificar ou destruir informações por pessoas que não têm legitimidade para tal. Ademais, instituiu a atuação de um comissário - eleito pelo parlamento – para vigiar os dados.

Já a Constituição espanhola prevê, em seu artigo 18, a proteção dos cidadãos frente o uso da informática. O dispositivo dispõe que haverá uma limitação legal quanto ao uso da informática para garantir a honra, intimidade e o exercício pleno de direitos.

Mais recentemente o Regulamento 2016/679 do Parlamento Europeu e do Conselho revoga àquela Diretiva e entra em vigor em 25 de maio de 2018. A norma, ão mais diretriz, tece novos contornos ao direito à proteção de dados pessoais pois incorpora no seu âmago a realidade da evolução tecnológica e da globalização. O Regulamento europeu introduz um novo modelo de gestão de proteção de dados que de acordo com José Luis Piñar Mañas significa:

---

[23] "Artigo 8º: Todas as pessoas em direito a proteção dos dados de caráter pessoal que lhes digam respeito.

1.Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento

da pessoa interessada ou com outro fundamento legitimo previsto por lei.

2.Todas as pessoas tem o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.

3.O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. "

> "Un nuevo modelo que podemos decir que pasa de la gestión de los datos al uso responsable de la información. Este es seguramente el más profundo cambio que el Reglamento va a imponern y que se aprecia en cuestiones como el princípio de *accountability* traducido por 'responsabilidad proactiva' (art. 5.2 del Reglamento), los princípios de privacidade desde el diseño y por el defecto, la aproximación de la proteccción de datos basada en el analisis de riesgo, la figura del Delegado de protección de datos, el fortalecimento de los códigos de conducta, la exigência de llevar un registro de las atividades del tratamento, la regulación de las medidas de seguridade"[24]

Sem adentrar em uma análise profunda do Regulamento europeu posto que não é objeto do trabalho, pode-se destacar o objetivo da nova norma relativamente a uniformização da legislação na UE e um nível elevado de proteção dos dados sobretudo porque o livre mercado está a exigir um maior número de transferência de dados impondo severas sanções para aqueles que descumprirem a norma[25]

Essas são algumas das novidades trazidas no campo da proteção de dados pessoais estabelecendo novas obrigações concernentes ao nível de responsabilidade levando em conta fatores como: a importância da proteção dos dados como direito fundamental, o direito ao controle do titular sobre seus próprios dados, sejam íntimos ou não, sempre que sejam ou venham a ser submetidos a tratamento, informatizado ou não (autodeterminação informativa), evolução tecnológica, livre circulação e mercado da UE e tendo aplicação extraterritorial, para além das fronteiras europeias quando a empresa internacional opere em território europeu.

---

[24] PINAR MANAS, Jose Luis.. Introducción. Hacia un Nuevo Moledo Europeo de Protección de Datos. **In:Reglamento General de Protección de DAtos – Hacia un nievo modelo de privacidade.** Editora Reus: Madrid.2016. p. 16.

[25] PINAR MANAS, José Luis. Introducción. Hacia un Nuevo Moledo Europeo de Protección de Datos. **In:Reglamento General de Protección de Datos – Hacia un nuevo modelo de privacidad.** Editora Reus: Madrid.2016. p.19.

3. A proteção de dados pessoais em conexão com a dignidade da pessoa humana e o livre desenvolvimento da personalidade para compreensão do ordenamento jurídico brasileiro.

O direito fundamental à proteção de dados pessoais no Brasil implica uma interpretação sistemática de nosso ordenamento jurídico a partir de um postulado básico, a dignidade da pessoa humana posto que os dados pessoais são direitos de personalidade.

Em estudo anterior,[26] a primeira autora deste ensaio já apontou que o princípio da dignidade da pessoa humana sendo basilar no sistema jurídico brasileiro posto que está previsto na Constituição Federal (CF/88, art. 1º, III) se revela como inerente ao próprio Estado Democrático de Direito, integrando sua estrutura. A dignidade da pessoa humana é fonte primária que apresenta as diretrizes do ordenamento jurídico dos Estados de Direito, representando vetor interpretativo e indicativo, e em se tratando do direito brasileiro, apresenta-se como um dos fundamentos do próprio Estado de Direito.

Salienta-se, também, que é perceptível e inegável a correspondência entre o princípio da dignidade da pessoa humana e os direitos fundamentais, aqui chamando a atenção para os direitos de liberdade, de intimidade, privacidade e proteção de dados pessoais, verificando-se assim uma vinculação entre os direitos e os princípios fundamentais.[27] E como se percebe a conexão da dignidade da pessoa humana com a privacidade? A partir de um conceito de dignidade da pessoa humana trazido por Ingo Sarlet[28] vê-se que:

> [...] por dignidade da pessoa humana *a qualidade intrínseca e distintiva reconhecida em cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer*

[26] RUARO, Regina Linden. Direito fundamental à liberdade de pesquisa genética e à proteção de dados pessoais: os princípios da prevenção e da precaução como garantia do direito à vida privada. Revista do Direito Público, Londrina, v. 10,, serie 2, 2015.

[27] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais.** 12ª ed. Porto Alegre: Livraria do Advogado. 2015a.

[28] SARLET, Ingo Wolfgang. **O princípio da dignidade da pessoa humana e os direitos fundamentais**. 2. ed. Porto Alegre: Livraria do Advogado, 2015b. p. 70

> *ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e corresponsável nos destinos da própria existência e da vida em comunhão com os demais seres que integram a rede da vida."*

O conceito do autor está em consonância com o que sustenta Stefano Rodotà quando compreende que a função sociopolítica da privacidade se projeta como elemento constitutivo da cidadania, figurando a dignidade, ao seu turno, como síntese dos princípios que visam a não redução da pessoa a fins mercadológicos, harmonizando-se com o respeito à igualdade e, principalmente, afastando a possibilidade de interferências não desejadas na vida do individuo:

> Projetada na sociedade, esta reconstrução das relações entre privacidade e dignidade se apresenta como fator fundamental para o contraste das potentes lógicas que impulsionam a transformação das nossas organizações sociais em sociedades de vigilância, da classificação, da seleção discriminatória. Uma tarefa, todavia, que parece se tornar cada vez mais difícil. [29]

Alexandre de Moraes[30] (2005, p. 128) conceitua a dignidade da pessoa humana da seguinte forma:

> A dignidade da pessoa humana é um valor espiritual e moral inerente à pessoa, que se manifesta singularmente na autodeterminação consciente e responsável da própria vida e que traz consigo a pretensão ao respeito por parte das demais pessoas, constituindo-se em um mínimo invulnerável que todo estatuto jurídico deve assegurar, de modo que apenas excepcionalmente possam ser feitas limitações ao exercício dos direitos fundamentais, mas sempre sem menosprezar a necessária estima que merecem todas as pessoas enquanto seres humanos.

As efetivações de políticas públicas de proteção de dados pessoais, em atenção às garantias fundamentais estabelecidas em um

---

[29] RODOTÁ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.. p. 237-238

[30] MORAES, Alexandre de. **Constituição do Brasil interpretada e legislação constitucional** 5ª edição. São Paulo: Atlas, 2005. p.128

Estado Democrático de Direito salientam ainda mais a estreita relação entre liberdade, privacidade e dignidade. Isso porque, sem dispor de uma robusta tutela das informações que digam respeito à pessoa – o que hoje, pode-se afirmar, constitui espécie de *corpo eletrônico* do ser humano[31] –, estará o Poder Público permitindo não só a intrusão de terceiros na sua esfera privada, mas também se omitindo na garantia de outros direitos fundamentais, como aqueles atinentes às condições de trabalho, acesso ao crédito e saúde.

Nessa perspectiva é que se insere a necessidade de uma lei que regule a proteção de dados pessoais garantindo a privacidade e a intimidade dos indivíduos estabelecendo sobretudo os princípios, direitos e deveres a serem respeitados por quem coleta os dados, os trata, refina criando os denominados "Big Data" e por fim, os comercializa, sem o conhecimento ou autorização do titular dos dados.

4. Panorama da indireta regulação do direito à proteção de dados pessoais no Brasil

Conforme já apontado no tópico anterior, não há um direito explícito e literal à proteção de dados pessoais no ordenamento pátrio o que não lhe retira a condição de direito fundamental. Tampouco o Brasil conta com uma lei específica em proteção de dados pessoais.[32] Feita essa ressalva, aponta-se que, muito embora não tenhamos norma, existem leis conexas com este direito que remetem a abrangência e seus limites a lei que ainda não foi promulgada.

Promulgada em 1988, a Constituição Federal apresentou técnica mais apurada e inovou ao reconhecer diversos direitos e garantias específicas. Em seu corpo normativo, abordou tanto a proteção dos direitos referentes ao cidadão como aqueles concernentes ao próprio Estado. Assim, o seu art. 1.º, III, ao reconhecer o princípio da dignidade humana, protegeu de imediato todos os direitos da personalidade, além de positivar garantias como a do direito à liberdade de expressão (art. 5º, inc. IX) e do direito à informação (art. 5º, inc. XV), a inviolabilidade da

31 Quanto a este conceito, Cf. RODOTÀ, 2008, p. 233.

32 Estão no Congresso Nacional aguardando para serem votados, dois Projetos de Lei, o PL 4060/12 e no Senado o PLS 181.

vida privada e da intimidade (art. 5º, inc. X), a garantia do Habeas Data (art. 5º, inc. LXXII), a proibição da invasão de domicílio (art. 5º, inc. XI) e violação de correspondência (art. 5º, inc. XII). [33]

No que concerne à identificação dos direitos da personalidade na Carta Política vigente, é fundamental salientar o apontamento feito por Gustavo Tepedino, no sentido de que não seria necessário que os direitos da personalidade fossem representados em um único direito subjetivo, ou ainda que fossem classificados múltiplos direitos da personalidade. A técnica mais apropriada seria a de, isto sim, proteger amplamente a pessoa humana em todos os seus aspectos. Destarte, pode-se afirmar que a dignidade seria o fundamento da República, configurando verdadeira cláusula geral de tutela e promoção da pessoa humana.[34] Nesta seara, ressalta-se, ainda, o atual entendimento de que os direitos fundamentais – que visam, juridicamente, a limitar o poder estatal, proibindo a interferência no plano individual dos cidadãos e, ao mesmo tempo, exigindo uma prestação estatal efetiva para a proteção desses direitos[35] – são autoaplicáveis no território brasileiro[36] e, portanto, o simples fato de inexistência de legislação específica que trate do direito à proteção de dados pessoais não pode constituir óbice para que se perfectibilize a sua defesa.

No plano infraconstitucional, integram este rol algumas disposições de natureza comercial e tributária, como o sigilo dos agentes do fisco (art. 198 do CTN), além das Leis 9.296/1996 e 10.217/2001, que tratam da interceptação telefônica e da gravação ambiental. Há, ainda, o Código de Defesa do Consumidor (Lei 8.078/1990), que trata dos bancos de dados nas relações de consumo, bem como a LC 105/2001, que

---

33 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. p. 323.

34TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro **Temas de Direito Civil.** 3. ed., rev. e atual. Rio de Janeiro : Renovar, 2004.. p. 47.

35 HAINZENREDER, Eugênio. O direito à intimidade e à vida privada do empregado frente ao poder diretivo do empregador: o monitoramento do correio eletrônico no ambiente de trabalho. Dissertação de Mestrado em Direito, Faculdade de Direito, PUC-RS. 2007. tede2.pucrs.br/tede2/bitstream/tede/4290/1/390730.pdf.

36 SARLET, Ingo. A eficácia dos direitos fundamentais. p. 243.

permite às autoridades administrativas a quebra do sigilo bancário, em certas situações, sem autorização judicial.[37]

Assume importância, para o estudo aqui realizado, o artigo 43 do Código de Defesa do Consumidor posto que elenca direitos e garantias para o consumidor em relação às suas informações pessoais contidas em bancos de dados e cadastros. As suas disposições focam no estabelecimento de equilíbrio nas relações de consumo através de interposição de limites ao fornecedor ao uso de informações sobre o consumidor. A imposição dessa restrição é importante para que o consumidor não perca sua liberdade individual, nem seja discriminado. Não se pode negar que o Código de Defesa do Consumidor trouxe inovações ao campo da proteção de dados pessoais, no entanto, devemos admitir que é uma tutela limitada às relações de consumo. Destaca-se que para muitos juristas, esse seria o marco normativo dos princípios de proteção de dados pessoais no Brasil[38].

Também cabe salientar que em novembro de 2011, foi promulgada a Lei de Acesso à Informação – lei n° 12.527 -, estabelecendo o livre acesso a informações, a exceção das informações pessoais e as informações sigilosas. Seu objetivo é garantir o máximo de transparência aos atos da Administração Pública.

Nosso ordenamento jurídico conta, também, com a Lei 12.965/14 - Marco Civil da Internet e seu regulamento o Decreto 8.771/16. Nestes diplomas normativos há expressa previsão da proteção de dados pessoal remetendo a uma legislação específica. Destarte, pode-se retirar o direito à autodeterminação informativa dos incisos X e XII do artigo 5º da Constituição,[39] que garantem, respectivamente, à

---

[37] LIMBERGER, Têmis. Proteção dos dados pessoais e o comércio eletrônico: os desafios do século XXI. *RDC* 67. p. 215-242.

[38] DONEDA, Danilo. *A proteção dos dados pessoais como um direito fundamental*. Espaço Jurídico, Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 103.

[39] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...] 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

inviolabilidade da intimidade e da vida privada; e o sigilo das comunicações em geral. De forma mais abstrata, pode-se entende-lo como uma forma de exercício do direito à liberdade previsto no *caput* do artigo 5º da Constituição Federal.

5. A concepção de dados pessoais como um direito fundamental no ordenamento jurídico brasileiro

Muito se discute acerca da existência de um direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro uma vez que não está previsto expressamente na Constituição Federal. Neste aspecto nos parece que, em favor de sua existência, Ingo Sarlet[40] bem argumenta ao defender que a mesma deriva de sua associação ao direito à privacidade "intimidade informática" e ao "livre desenvolvimento da personalidade, que inclui o direito à livre disposição sobre os dados pessoais"

Ingo Sarlet[41] ensina que o direito a proteção de dados pessoais abarca as seguintes posições jurídicas:

> [...] a) o direito de acesso e conhecimento dos dados pessoais existentes em registros (bancos de dados) públicos e privados; b) direito ao não conhecimento, tratamento e utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, aqui incluído um direito de sigilo quanto aos dados pessoais; c) direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados; d) o direito ao conhecimento da finalidade da coleta e eventual utilização dos dados; e) direito a retificação e, a depender do caso, de exclusão de dados pessoais armazenados em banco de dados.

Reforça, também, que tal direito abarca a autodeterminação informativa, matéria esta que será tratada em outro apartado dada a relevância do tema na crítica à Decisão do TJRS referida na Introdução deste artigo.

---

forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

40 MARINONII, Luiz Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. *Curso de Direito Constitucional*. São Paulo: Revista dos Tribunais, 2014. p. 433/434

41 MARINONII, Luiz Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. *Curso de Direito Constitucional*. São Paulo: Revista dos Tribunais, 2014. p. 434/435

Danilo Doneda[42] argumenta que existe uma menção ao caráter de direito fundamental da proteção de dados pessoais na Declaração de Santa Cruz de La Sierra, documento final da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, firmada pelo governo brasileiro em 15 de novembro de 2003. No item 45 da Declaração tem-se que:

> Estamos também conscientes de que a proteção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidos na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Proteção de Dados, aberta a todos os países da nossa comunidade.

Cabe salientar, ainda, que nem todo o dado é considerado dado pessoal para efeitos de proteção legal específica. Um dado, para caracterizar-se como pessoal, deve ter certas características. A fundamental delas é ter um vínculo objetivo com uma pessoa, é revelar um aspecto objetivo de seu titular.

> Este vínculo significa que a informação se refere às características ou ações desta pessoa, que podem ser atribuídas a ela em conformidade à lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como sobre opiniões que manifesta e tantas outras[43].

Assim, pode-se dizer que os dados pessoais são uma "continuação por outros meios" do direito fundamental à privacidade, isto é, um desdobramento da tutela do direito à privacidade [44] e têm a capacidade ou o potencial de nos identificar, de demonstrar as características da personalidade de uma pessoa; esta é a razão pela qual estão substancialmente ligados à privacidade, pois maior será a

---

42 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico. Joaçaba, v. 12, n. 2, jul./dez. 2011. p. 103.

43 DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico, Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 93.

44 DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006.

privacidade do sujeito à medida que for menor a difusão de suas informações pessoais.

Diante disso, surgem preocupações quando dados pessoais são utilizados para a formação de Big Datas, pois através da coleta, do tratamento e da transferência destes é possível conhecer a personalidade, as atividades públicas e privadas, perfil, etc, muitas vezes, invadindo uma esfera estritamente pessoal de seu titular por natureza, o indivíduo.

A coleta de informações não é fruto da sociedade da informação[45] - ela é uma prática milenar. O seu destaque nos dias de hoje – e apreensão – se dá devido à alta desenvoltura da manipulação, além de que na maioria das vezes, o cidadão não tem conhecimento dessas atividades (invasoras). Na medida em que cresce a capacidade de armazenar, tratar e comunicar as informações, aumentam as maneiras pelas quais os dados podem ser utilizados, isto é, a coleta para fins lícitos, como na prevenção de delitos ou na celebração de um contrato com plenos conhecimentos de causa. Em contrapartida, também pode ser utilizada para fins contrários ao Direito e à moral, como a perseguição política ou a opressão econômica[46]. É que esta coleta dá azo a um sem fim de Big Datas que nada mais são do que um conjunto de informações estruturadas de acordo com uma determinada lógica utilitarista, isto é, faz-se a máxima extração possível de um conjunto de informações.

Por outro lado, o tratamento de dados pessoais se dá principalmente por meios automatizados, isto é, utiliza-se de meios informáticos para realizar o processamento de dados. Porém, não há correção da resposta no sistema, o que torna esse processamento uma atividade de risco. No âmbito de proteção de dados pessoais, o perigo se concentra na exposição e utilização indevida e/ou abusiva das informações, tendo em vista que elas podem ser incorretas, de modo a representar erroneamente seu interessado[47]. Por outro lado, o uso de dados pessoais pode não ser de conhecimento de seu titular enquanto

---

[45] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **In: Espaço Jurídico**, Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 92.

[46] STJ, Recurso Especial n. 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995, p. 6119.

[47] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **In: Espaço Jurídico**, Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 93.

diferentemente do direito à privacidade porque este quando desrespeitado vem à tona, torna-se de conhecimento público. É, justamente, por tal motivo que deve haver uma proteção especial do Direito que garanta o respeito aos princípios para coleta, tratamento e transferência.

Em face do panorama brasileiro, caber, então, ao Poder Judiciário tutelar a pretensão daqueles que pretendam ver seus dados pessoais protegidos, quer seja na relação de particulares, quer seja na seara do direito público tarefa esta que enseja uma interpretação sistemática a partir da Constituição Federal, dos diplomas legais existentes e dos princípios informadores.

6. Importância da proteção de dados pessoais especial relevância do princípio da finalidade e da autodeterminação informativa como corolários da dignidade da pessoa humana

O princípios específicos da proteção de dados pessoais têm importância fundamental na garantia de tal direito e foram previstos em documentos internacionais constituindo-se em vetores para sua consecução, sobretudo quando se trata de um país como o Brasil que carece de legislação específica.

Laura Mendes assevera que:

> A convergência internacional estabelecida acerca dos princípios é marcante: mesmo os ordenamentos jurídicos mais diversos preveem praticamente os mesmos princípios de proteção de dados, com mínimas diferenças. Esse quadro comum de princípios é conhecido por "*Fair Information Principles*" e teve sua origem na década de 70 de forma quase simultânea nos Estados Unidos, Inglaterra e Alemanha.[48]

A espinha dorsal da proteção de dados pessoais, é, basicamente, formada por cinco princípios, a saber: a) princípio da publicidade: a existência de banco de dados deve ser de conhecimento do público; b) princípio da exatidão: as informações devem ser fiéis à realidade e deve

[48] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental.** Saraiva: São Paulo. 2014. p. 68.

haver a possibilidade de atualizá-las periodicamente; c) princípio da finalidade: utilizar os dados para fins determinados - o qual deve ser comunicado ao titular antes da coleta; d) princípio do livre acesso: o interessado deve poder ter acesso aos ficheiros que contêm seus dados, além de poder controlá-los – de acordo com o princípio da exatidão; e) princípio da segurança física e lógica: os dados devem ser protegidos contra extravios, destruições, modificações, transmissões ou acessos não autorizados[49]. Para garantir o respeito a tais princípios é que diversos países têm uma legislação específica acerca da proteção de dados pessoais.

Assume relevância em matéria de proteção de dados pessoais o princípio da finalidade resulta que os dados pessoais ao serem coletados são ou devem ser a título de um fim específico, ou seja, "indica a correlação necessária que deve existir entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta dos dados".[50] Esse princípio resguarda o titular dos dados de uso por terceiros não legitimados na relação estabelecida com quem coleta os dados pessoais. Assim, por exemplo, se a coleta dos dados pessoais têm por finalidade a formação de um banco de dados finalidade de proteção ao crédito para o mercado (SPC e SERASA), ainda que possa ser disseminada para aqueles que têm a mesma finalidade, não poderá se-lo para fins alheios ao objetivo sem o prévio consentimento livre, informado e específico. A razão do princípio da finalidade como fundamental para o direito à proteção de dados pessoais se constitui no que convencionou-se chamar de autodeterminação informativa, sendo esta um desdobramento do direito à privacidade, podendo ser chamado, também, de direito à "privacidade informacional."[51]

A autodeterminação informativa resguarda o titular dos dados contra a utilização indevida de suas informações, coibindo

---

[49] DONEDA, Danilo. *A proteção dos dados pessoais como um direito fundamental.* Espaço Jurídico, Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 100-101.

[50] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: Linhas Gerais de um novo direito fundamental.** São Paulo: Editora Saraiva. 2014. p. 70.

[51] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação, efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Sergio Antonio Fabris Editor, 2007. p. 27

discriminações e controles sociais calcados em bancos de dados que não são de seu conhecimento busca-se assegurar o respeito à dignidade da pessoa humana. Danilo Doneda[52], ensina que o direito à autodeterminação informativa tem *status* de direito fundamental por tratar-se de direito de personalidade, o que garante, de *per si,* ao indivíduo, o poder de controlar as suas próprias informações. Ou seja, seria uma afirmação do personalíssimo no âmbito das interações entre indivíduo e sociedade. Neste sentido, constitui-se na liberdade que o titular dos dados tem de dispor de suas informações pessoais, consoante seu próprio interesse. É o direito que tem o individuo de escolher com quem pretende compartilhar suas informações, partindo do pressuposto de que pode vetar qualquer ingerência não consentida e porquanto são dados e informações de caráter pessoal[53] que quer manter em sigilo.

A exemplo de outros direitos fundamentais, a autodeterminação informativa não possui um caráter absoluto, podendo ser limitada quando em conflito com outro direito fundamental ou diante de previsão constitucional. "Assim, a proteção dos dados pessoais é a regra, e a intervenção estatal se dá em casos excepcionais."[54] É com base na dignidade da pessoa humana e dos direitos de personalidade que a noção de autodeterminação informativa deve estar muito mais atrelada ao ser humano do que ao controle da informação em si. Nesse aspecto, elucidam Antoinette Rouvroy e Yves Poullet:

---

52 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

53 Entende-se por informações pessoais aquelas que possuam um vínculo objetivo com a pessoa a qual diga respeito, dizendo respeito a suas características ou a suas ações. "É importante estabelecer esse vínculo objetivo, pois ele afasta outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais." (DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. **Espaço Jurídico: Journal of Law [EJJL]**, [S.l.], v. 12, n. 2, p. 91-108, Dez. 2011. ISSN 2179-7943. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658>. Acesso em: 09 out. 2014.)

54 RODRIGUEZ, Daniel Piñeiro. **O direito fundamental à proteção de dados pessoais: as transformações da privacidade na sociedade de vigilância e a decorrente necessidade de regulação**. 2010. 153 f. Dissertação de Mestrado – Programa de Pós-Graduação em Direito, Pontifícia Universidade Católica do Rio Grande do Sul. Porto Alegre, 2010. p. 60.

> Informações e dados não são os 'elementos' ou os 'blocos construtores' pré-existentes de uma personalidade individual ou 'própria'. [...] O que a expressão 'autodeterminação informacional' significa, mais que o controle do indivíduo sobre as informações e dados produzidos sobre si, uma (necessária mas insignificante) pré-condição para que ele viva uma existência que pode ser dita como 'autodeterminada'.[55]

Portanto, é desse direito que decorre a necessidade de prévio consentimento do titular para a coleta e tratamento de seus dados pessoais. Corroborando com o entendimento temos Iglesias Fernanda de Azevedo Rabelo e de Filipe Rodrigues Garcia:

> O titular das informações pessoais, ao dispor de parte de sua esfera privada, concordando em ceder seus dados a terceiro, legitima a atividade de coleta e tratamento dos dados. Isso porque o titular é o único que poderá avaliar os efeitos da circulação de suas informações. O consentimento prévio, assim, mostra-se como um requisito de validade à atividade de coleta de dados privados.[56]

Ainda, o consentimento deve vir precedido dos devidos esclarecimentos sobre quais dados serão coletados, de que forma se dará o tratamento, com quem eles serão compartilhados e para qual finalidade. Caso o coletador/possuidor dos dados pretenda utilizá-los para fim diverso, será necessário obter novo consentimento.

No ordenamento jurídico brasileiro, não há previsão expressa ao direito à autodeterminação informativa, entretanto, tal situação não pode ser interpretada no sentido de inexistir tutela jurídica no País. Vale lembrar que os princípios constitucionais não necessariamente têm previsão expressa na Constituição Federal, podendo "derivar da

---

55 ROUVROY, Antoinette e POULLET, Yves. *The Right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy*. p. 51. In: GUTWIRTH, Serge et al. Reinventing Data Protection? Sispringer, 2009.

Information and data are not the pre-existing 'elements' or 'building blocks' of an individual's personality or 'self. […] What the expression 'informational self-determination' means is rather that an individual's control over the data and information produced about him is a (necessary but insufficient) precondition for him to live an existence that may be said 'self-determined'. (Tradução Nossa)

56 RABELO, Iglesias Fernanda de Azevedo e GARCIA, Filipe Rodrigues. **O direito à autodeterminação informativa**. Disponível em <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10473> Acesso em: 07 out 2014.

interpretação do sistema constitucional adotado ou [...] brotar da interpretação harmonizadora de normas constitucionais específicas."[57]

7. Dado pessoal e Livre Mercado

Após discorrer sobre o direito à proteção de dados pessoais enquanto direito fundamental no sistema constitucional brasileiro e trazer um panorama da matéria no sistema americano e europeu, cabe, agora, tecer uma análise de uma das consequências derivadas da ausência da lei específica de proteção de dados pessoais no Brasil cujo conteúdo de tal direito passou a ser delimitado pela jurisprudência dos Tribunais.

No caso concreto, pretende-se debater a recente Decisão do Tribunal de Justiça do Rio Grande do Sul na Ação Coletiva[58] impetrada pelo Ministério Público em face da Confederação Nacional de Dirigentes Lojistas – SPC BRASIL com base no caráter abusivo da comercialização dos dados e informações pessoais dos consumidores.

Nos fundamentos da propositura da Ação Coletiva o Ministério Público arguiu a afronta aos direitos fundamentais protegidos pelo artigo 5º, inciso X da Constituição Federal[59] considerando, ainda, haver uma prática abusiva por parte das empresas e na finalidade da formação dos bancos de dados dos consumidores que se destina à prospecção de clientes, ações de marketing e telemarketing, através de malas diretas, telefonemas e mensagens oferecendo produtos e serviços. Os dados pessoais coletados consistem em: "nome completo, telefone, endereço, número de documentos de identificação, data de nascimento, nomes dos pais, e-mails, dentre outras informações pessoais."[60] não houve oposição

---

[57] LÔBO, Paulo. **A nova principologia do direito de família e suas repercussões**. IN: HIRONAKA, Giselda Maria Fernandes; TARTUCE, Flávio; SIMÃO, José Fernando. Direito de família e das sucessões: temas atuais. Rio de Janeiro: Forense; São Paulo: Método, 2009, p. 3.

[58] Apelação Cível 70069420503, Sexta Câmara Cível, Relator Des. Ney Weidmann Neto.www..tjrs.jus.br. Acesso em: 13/03/2017.

[59] **Art. 5º X** - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

[60] www.tjrs.jus.br. Acesso em 13/03/2017.

à formação de banco de dados de consumidores para fins de avaliação de crédito.

No que atine ao objeto específico do presente estudo, dentre os requerimentos do Ministério Público se encontram: a) o cancelamento dos registros que não tenham sido autorizados pelos titulares dos dados; b) a abstenção de comercializar e de divulgar os dados de consumidores sem o prévio consentimento dos mesmos e, c) que o registro cadastral e informações pessoais nos bancos de dados de suas responsabilidades esteja condicionado à prévia autorização do titular dos dados.

Em sua defesa, os argumentos da ré invocaram a importância da formação dos bancos de dados de consumidores para a economia, a legalidade da comercialização de dados de "mera identificação social" e a desnecessidade de consentimento prévio do titular. Ainda, dentre as alegações, foi levantada a questão de que os dados pessoais são públicos e encontrados na internet daí o porquê de não estarem sujeitos ao sigilo.

Na base do Acórdão referido encontra-se a discussão acerca do grau de privacidade ao qual os dados cadastrais gozam. O Relator entendeu que os dados coletados e comercializados apesar de serem privativos, "são comumente fornecidos por qualquer cidadão na prática dos atos da vida civil, não se tratando de informações de natureza totalmente sigilosa ou confidencial, Não há, no caso, qualquer ofensa à privacidade ou a qualquer outro direito fundamental dos consumidores."[61]

Percebe-se de imediato a tensão entre o Direito e Inovação, este último consubstanciado no manejo das novas tecnologias a serviço do livre Mercado. Para melhor entender onde se manifesta tal tensão é preciso que se aponte que um dado pessoal isolado, por exemplo o CPF, é de extrema importância, uma vez que enseja que um determinado indivíduo seja imediatamente identificado. No entanto, o dado isolado não é capaz de produzir um perfil. Assim, o problema se apresenta quando são coletados, cruzados, tratados vários dados pessoais de um mesmo indivíduo (ainda que sejam dados públicos) e depositados em um Banco de dados, porquanto são capazes de fornecerem uma visão

[61] Tal afirmação se encontra a fls. 11 do Acórdão. Acesso em 15/03/2-17.

geral de uma pessoa em específico.[62] A partir do mento que o dado é coletado, torna-se uma informação de vez que "estabelece um vínculo objetivo com a pessoa revelando aspectos dessa".[63]

Com o tratamento que recebem em face de operações técnicas tornam-se valiosos e por tal razão merecem a tutela jurídica do Direito. Com a inovação possibilita-se o possibilita o tratamento de dados por meios informatizados que afetam a privacidade do titular dos dados.[64]

Laura Mendes analisando a aponta que:

> [...] a informatização dos meios para o tratamento de dados pessoais afetou o direito à privacidade do indivíduo principalmente por duas razões: i) ao ampliar a possibilidade de armazenamento, tornando-a praticamente ilimitada; ii) ao possibilitar a obtenção de novos elementos informativos por meio da combinação de dados em estado bruto, a princípio, desprovidos de importância, a partir da utilização de novas técnicas, tais como o '*profiling*', '*data mining*', '*data warehousin', 'scoring-system'* dentre outros".[65]

Assim, em análise à doutrina, tem-se que pese a menção expressa do não ferimento ao direito à fundamental privacidade, contida no Acórdão, esta não é a melhor interpretação. Extrai-se, também, do texto que outros elementos centrais como por exemplo, o direito à autodeterminação informativa no que concerne à venda de dados pessoais para ações de marketing com vistas a prospecção de clientes pelas empresas associadas porque desconectados da finalidade de sua coleta pelos órgãos de proteção ao crédito. Este tópico merece uma análise mais acurada.

---

[62] SARMENTO E CASTRO, Catarina. **Direito da Informática, privacidade e dados pessoais.** Coimbra: Almedina. 2005. p.81.

[63] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. **Da privacidade à proteção dos dados pessoais.** Rio de Janeiro: Renovar, 2006.p. 157

[64] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental.** Saraiva: São Paulo. 2014. p. 58-59.

[65] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental.** Saraiva: São Paulo. 2014. p. 59-60.

O ordenamento jurídico brasileiro permite a existência de bancos de dados destinados ao consumo conforme se depreende o artigo 43 do CDC:

> O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> §1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> §2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

Não obstante a desnecessidade de prévio consentimento do afetado pela coleta de dados, em interpretação sistemática com conteúdo do direito fundamental à proteção de dados, há de se ter em conta a finalidade de sua coleta. Neste sentido, torna-se imprescindível verificar a natureza da criação dos órgãos que colhe, tratam e transferem os dados.

O SPC e o SERASA, é sabido, foram criados para proteger as empresas da inadimplência dos consumidores[66], são órgãos de proteção ao crédito e por sua natureza, para esta finalidade, prescindem de autorização do consumidor para coleta de dados pessoais que nesta categoria não se consideram como sigilosos podendo ser coletados e de caráter público dentre os associados aos sistemas devendo preservar sua natureza apenas informacional. Assim, usá-lo para fins de prospecção de clientes, marketing, etc, constitui-se em finalidade alheia à sua natureza e portanto torna-se inconstitucional.

Veja-se a atividade do SPC informada em sua página oficial:

> O SPC Brasil é o sistema de informações das Câmaras de Dirigentes Lojistas – CDL, constituindo–se o mais completo banco de dados da América Latina em informações creditícias sobre pessoas físicas e pessoas jurídicas, auxiliando na tomada de decisões para concessão de crédito pelas empresas em todo país.

[66] SPC – Serviço de Proteção ao Crédito

> Por meio do SPC Brasil, o usuário tem acesso aos bancos de dados de mais de 2.200 Entidades presentes em todas as capitais e nas principais cidades de todos os estados.
> A capilaridade alcançada pelo SPC Brasil é a mais representativa do setor, reunindo informações do comércio nacional, desde os pequenos lojistas até os grandes magazines, indústrias, serviços e mercado financeiro.
> Hoje, 1, 2 milhão de empresas associadas às Entidades em todo o Brasil usufruem de soluções que atendem a cada necessidade do ciclo de negócios das empresas, oferecidas pelo SPC Brasil.
> Com o objetivo de contribuir de maneira relevante para o desenvolvimento do mercado de consumo, o SPC Brasil está há mais de 55 anos ajudando empresas de todos os portes e segmentos a crescer e também concedendo crédito a muitos brasileiros, promovendo o desenvolvimento econômico do Brasil.[67]/[68]

Por outro lado, o Acórdão, a fls. 11, cita, literalmente, uma passagem da doutrina[69] ao qual os ensinamentos fundamentam a legalidade da formação de banco de dados de proteção ao crédito e releva a importância de que as mesmas tenham a finalidade de analisar o crédito ao consumidor.[70]

No entanto, em que pese o esforço da Decisão em pretender amparar a legalidade de comercialização de banco de dados pessoais para o fim de propiciar uma ação de marketing ou outras para prospecção de clientes, no que se depreende do Acordão, há uma

---

[67] https://www.spcbrasil.org.br/institucional/spc-brasil. Acesso em: abril 2017.

[68] A Serasa Experian e o Serviço de Proteção ao Crédito são duas empresas prestadoras de serviços responsáveis por registrar, em um gigantesco banco de dados, o nome completo e o CPF de um indivíduo que possua dívidas vencidas. O banco de dados fomentado pelas credenciadas será disponibilizado para os comerciantes que contratarem os seus serviços. Com a contratação, as informações registradas no banco de dados são repassadas ao empresário contratante e servirão de critério para concessão de crédito para o indivíduo. https://bhpatricio.jusbrasil.com.br/artigos/172171733/diferencas-entre-orgaos-de-protecao-ao-credito-spc-serasa-cobrancas-de-dividas-inexistentes-e-os-direitos-do-consumidor. Acesso em: abril de 2017.

[69] Vide "Manual de direito do consumidor, 1ª ed. Revista dos Tribunais de autoria de Antonio Hermann Benjamin, Claudia Lima Marques e Leonardo Roscoe. Ano de 2013.

[70] Nesse sentido dispõe o artigo 3º, §3º, I da Lei 12.414/2011 ao tratar de informações excessivas dispondo: "assim consideradas aquelas que não estiverem vinculadas à análise de crédito ao consumidor"

incongruência entre o fundamento teórico da doutrina citada e do que ele dispõe conforme segue:

> Importante registrar que as informações que a ré comercializa, tais como, por exemplo, nome, data de nascimento, idade, CPF, são disponibilizadas tão somente a pessoas jurídicas e profissionais liberais assinantes do serviço, com a finalidade, indiscutivelmente, apenas empresarial, não se tratando de informação que viole a privacidade do indivíduo.[71]

Efetivamente, a coleta de tais dados não afrontam o direito à privacidade das partes envolvidas na relação ou terceiros – empresas e profissionais associados ao sistemas sempre e quando seja para a finalidade de proteção ao crédito, devendo, apenas, haver a informação comunicada por escrito ao consumidor, nos temos do artigo 43, parágrafo segundo do CDC, prescindindo, inclusive, de prévio consentimento. Diferentemente se opera quando se tratar de atividade com a finalidade "empresarial". Primeiro, porque esta expressão e atividade são por demais vagas e abarcam finalidades estranhas às próprias do sistema já apontados anteriormente. Segundo, porque na sociedade das tecnologias avançadas - TIC, o sistema cada vez mais refinado de coleta e tratamento de dados tem possibilitado a manipulação que pode resultar em formação de perfis.

Laura Mendes, muito acertadamente alerta para o risco da formação de perfis (*Profiling)* ao ensinar que:

> Os riscos da técnica de construção de perfis não residem apenas na sua grande capacidade de junção de dados; na realidade, a ameaça consiste exatamente na sua enorme capacidade de combinar diversos dados de forma inteligente, formando novos elementos informativos.[72]/[73]

---

[71] Apelação Cível 70069420503, Sexta Câmara Cível, Relator Des. Ney Weidmann Neto.www..tjrs.jus.br. fls. 13. Acesso em: 28/03/2017.

[72] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental.** Saraiva: São Paulo. 2014. p. 111.

[73] Segundo Laura Mendes, na mesma obra, aponta vários mecanismo de de técnicas de processamento de dados, por exemplo Data warehousing, Data mining, Online Analytical Processing, Profiling,Scoring.

Nessa lógica, o ser humano sai da sua condição de sujeito para tornar-se objeto - objeto de valor comerciável o que resulta na afronta direta do principio da dignidade da pessoa humana.

A decisão jurisprudencial reconhece que os dados pessoais são privativos, porém, mitiga tal qualificativo ao afirmar expressamente:

> [...] ainda que, sem sombra de dúvida, privativos, são comumente fornecidos por qualquer cidadão na prática dos atos da vida civil, não se tratando de informação de natureza totalmente sigilosa ou confidencial. Não há, no caso, qualquer ofensa à privacidade ou a qualquer ofensa à privacidade ou a qualquer outro direito fundamental.[74]

Em verdade, ainda que os dados pessoais sejam fornecidos pelos seus titulares, estes ocorrem para determinada finalidade específica e não para, sem consentimento, serem aplicados em outras e se tornem objeto de comércio. Aqui não se está falando de privacidade mas, mais bem, de autodeterminação informativa necessária quando excede os fins da coleta e dos princípios da proteção de dados pessoais, portanto, em tais situações não há como afastar a afronta aos princípios e direitos fundamentais já apontados nos tópicos anteriores. Não é por outra razão que o intento de compatibilizar a existência da privacidade com o mercado é um desafio importante. Se de um lado tem-se a livre iniciativa econômica, de outro temos a dignidade da pessoa humana. Neste particular, com propriedade Fernanda Barbosa[75] ao tratar do tema traz à baila a distinção realizada por Kant no Século XVIII quando aquele filósofo distinguiu "coisas" e "pessoas", afirmando que existem duas categorias de valores: o preço e a dignidade.

Assim, a ausência de legislação específica em matéria de proteção de dados pessoais tem ensejado as mais diversas interpretações dos Tribunais que, ao invés de resolverem os dilemas antes apresentados, aumentam a tensão social coisificando o ser humanos e fortalecendo o império econômico.

---

74 Apelação Cível 70069420503, Sexta Câmara Cível, Relator Des. Ney Weidmann Neto.www..tjrs.jus.br. fls. 11. Acesso em: 13/03/2017.

75 BARBOSA, Fernanda Nunes. Informação e Consumo: A proteçãoo da privacidade do consumidor no mercado contemporâneo da oferta. **In:Direito Privado e Internet.** Org. Guilherme Magalhães Martins. São Paulo: Editora Atlas. 2014. p.237-257

Considerações finais

A matéria da proteção de dados pessoais engloba temas relacionados ao direito à privacidade, seu porto de origem, todavia ela acaba extrapolando este âmbito. A proteção a dados pessoais objetiva promover a funcionalidade de alguns valores fundamentais do ordenamento. A normatização desta área pode até parecer uma intromissão a um domínio já pacificado; mas esse é mais um caso em que a tecnologia é capaz de modificar situações estáveis. Deve-se estabelecer um regime de proteção aos dados pessoais idêntico para o Estado e para os entes privados. Além disso, em decorrência da maleabilidade e velocidade da tecnologia da informação, necessita-se de uma disciplina que não seja única, que não se esgote em soluções pontuais e concretas.

Em relação ao Brasil, o estudo concluiu que a nossa legislação está carente quando se trata de proteção de dados pessoais. A tutela oferecida pelos institutos esparsos é insuficiente,. Além disso, ele tem caráter estritamente remedial, isto é, pós-fato; não há cunho preventivo. O Código de Defesa do Consumidor trouxe inovações, porém, restritas às de relações de consumo.

A tensão entre direitos fundamentais e mercado tende a aumentar na medida em que as pessoais se tornam objeto de comércio e estão à mercê de interesses econômicos privados cujas finalidades, por vezes, são desconhecidas ou estranhas às relações pactuadas que sobrelevam o consumo em detrimento do consumidor.

Referências bibliográficas

Apelação Cível 70069420503, Sexta Câmara Cível, Relator Des. Ney Weidmann Neto.http://www.tjrs.jus.br. Acesso em: 28/03/2017.

BARBOSA, Fernanda Nunes. Informação e Consumo: A proteçãohn da privacidade do consumidor no mercado contemporâneo da oferta. **Direito Privado e Internet.** Org. Guilherme Magalhães Martins. São Paulo: Editora Atlas. 2014

BENJAMIN, Antonio Hermann. MARQUES, Claudia Lima. ROSCOE, Leonardo. **Manual de direito do consumidor**, 1ª ed. Revista dos Tribunais. 2013.

DECLARAÇÃO DE SANTA CRUZ DE LA SIERRA. Disponível em : <http://www.segib.org/documentos/por/DECLARASAO-STA-CRUZ-SIERRA.pdf> Acessado em 19 mar. 13

DIRETIVA 46/95/CE. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pt:HTML>. Acessado em: fev. 2016.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico.** Joaçaba, v. 12, n. 2, jul./dez. 2011.

_____. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006.

HAINZENREDER, Eugênio. O direito à intimidade e à vida privada do empregado frente ao poder diretivo do empregador: o monitoramento do correio eletrônico no ambiente de trabalho. **Dissertação de Mestrado em Direito**, Faculdade de Direito, PUC-RS. 2007. Acesso em: http://www.ede2.pucrs.br/tede2/bitstream/tede/4290/1/390730.pdf.

LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção de dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

LIMBERGER, Têmis. Proteção dos dados pessoais e o comércio eletrônico: os desafios do século XXI. **RDC** 67

LÔBO, Paulo. A nova principiologia do direito de família e suas repercussões. HIRONAKA, Giselda Maria Fernandes; TARTUCE, Flávio; SIMÃO, José Fernando. **Direito de família e das sucessões: temas atuais**. Rio de Janeiro: Forense; São Paulo: Método, 2009.

MARINONI, Luiz Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. **Curso de Direito Constitucional**. São Paulo: Revista dos Tribunais, 2012.

MARTÍNEZ, Ricardo Martínez. **Una aproximación crítica a la autodeterminación informativa**. Madrid: Thomson Civitas, 2004.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental.** Saraiva: São Paulo. 2014.

MILLS, Jon L. **Privacy: the lost right**. New York: Oxford University Press, 2008.

RABELO, Iglesias Fernanda de Azevedo e GARCIA, Filipe Rodrigues. **O direito à autodeterminação informativa**. Disponível em <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10473> Acesso em: 07 out 2014.

PINAR MANAS, Jose Luis.. Introducción. Hacia un Nuevo Moledo Europeo de Protección de Datos. **Reglamento General de Protección de Datos – Hacia un nuevo modelo de privacidade.** Editora Reus: Madrid.2016.

REINALDO FILHO, Demócrito. A Diretiva Europeia sobre proteção de dados pessoais. Uma análise de seus aspectos gerais. **In: Jus Navigandi**. Teresina: ano 18, n. 3507. 6fev. 2013. Disponível em: <http://jus.com.br/revista/texto/23669>. Acesso em: fev. 2013.

RODOTÁ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIGUEZ, Daniel Piñeiro. O direito fundamental à proteção de dados pessoais*:* as transformações da privacidade na sociedade de vigilância e a decorrente necessidade de regulação. Porto Alegre: PUCRS, 2010, 168f. **Dissertação de Mestrado (Mestrado em Direito) -**Faculdade de Direito, PUCRS, Porto Alegre, 2010.

ROUVROY, Antoinette e POULLET, Yves. The Right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. p. 51. **GUTWIRTH, Serge et al. Reinventing Data Protection?** Sispringer. 2009

RUARO, Regina Linden. Responsabilidade civil do Estado por dano moral em caso de má utilização de dados pessoais. **Direitos Fundamentais e Justiça***.* Porto Alegre: PUCRS, 2007. Vol.1.

_____; RODRIGUEZ, Daniel P.; FINGER, Brunize. O direito à proteção de dados pessoais e à privacidade. **Revista da Faculdade de Direito da UFPR.** Curitiba: UFPR, 2011.Vol. 53.

SARMENTO E CASTRO, Catarina. **Direito da Informática, privacidade e dados pessoais.** Coimbra: Almedina. 2005.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. **Temas de Direito Civil.** 3. ed., rev. e atual. Rio de Janeiro : Renovar, 2004.

TAVARES, André Ramos. **Curso de Direito Constitucional**. 8ª edição. São Paulo: Editora Saraiva, 2010.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação, efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Sergio Antonio Fabris Editor, 2007

WARREN, Samuel D. BRANDES, Louis D. The Right to Privacy**. Harvard Law Review**, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220. Disponível em: <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>. Acesso em: Março de 2017.

A TROCA INTERNACIONAL DE INFORMAÇÕES FISCAIS E OS DIREITOS DO CONTRIBUINTE

Paulo Caliendo[*]

Introdução

O presente artigo tem por problema verificar a atualidade, conceito e extensão do conceito de troca de informações, para fins fiscais e os direitos do contribuinte. Cada vez mais tem sido questionada a legitimidade da manutenção do sigilo fiscal, como um verdadeiro direito do contribuinte, apresentando-se, de outro lado, como uma ofensa horizontal aos direitos de outros contribuintes. A própria lei manteria um caráter prejudicial ao garantir a determinados contribuintes o direito de ocultar os seus rendimentos, perante a grande maioria dos contribuintes, que possuem transparência fiscal efetiva, em face dos rendimentos que possuem. Assim assalariados, pequenos empresários e prestadores de serviços estariam sendo penalizados, frente aos detentores de rendimentos financeiros em países com tributação favorecida ou aplicados em empresas estrangeiras off-shore. O texto pretende verificar o estado atual dessa discussão no Direito Internacional e sua repercussão no Direito nacional.

A troca de informações fiscais na experiência internacional

O debate sobre o sigilo bancário, para fins fiscais, recebeu um grande desenvolvimento a partir de 2000 e, especialmente, após a crise de 2008. Nesse momento é criado o *Global Forum on Transparency and Exchange of Information for Tax Purposes*, sob os auspícios da

[*] Doutor em Direito pela Pontifícia Universidade Católica de São Paulo (2002), Doutorado Sandwich na Ludwig-Maximilians Universität em Munique (Alemanha) (2001). Mestre em Direito pela Universidade Federal do Rio Grande do Sul (1996). Graduado em Direito pela Universidade Federal do Rio Grande do Sul (1992). Participou do Program of Instruction for Lawyers da Harward Law School (2001). Árbitro da lista brasileira do Sistema de Controvérsias do Mercosul. Atualmente, é professor permanente da Pontifícia Universidade Católica do Rio Grande do Sul. Autor da obra finalista do Prêmio Jabuti "Direito Tributário e Análise Econômica do Direito" e da obra "Direito Tributário: três modos de pensar a tributação". Endereço para acessar este CV Lattes: <http://lattes.cnpq.br/9047483160060734>. E-mail: p.caliendo@terra.com.br.

Organização para Cooperação e Desenvolvimento Econômico (OCDE). Esse é entendido como uma rede multilateral para implementar políticas de transparência e troca de informações, para fins fiscais. Um dos seus objetivos é estabelecer *standards* internacionais para implementação da transparência fiscal[1].

Um dos objetivos desse fórum é o estabelecimento de assistência técnica aos membros da Organização. Existem dois standards internacionalmente aceitos: a t*roca de informações mediante requisição* (*Exchange of Information on Request* -EOIR) e a *troca automática de informações* (*Automatic Exchange of Information* - AEOI). Existem mais de uma centena de países adeptos da implementação de cada um desses standards, e os números são crescentes[2]. São objetivos desses planos a luta contra a evasão fiscal (*fight against tax evasion*), bem como a cooperação internacional entre as administrações tributárias.

Diversas jurisdições irão iniciar a troca automática de informações em 2017[3] e outra parte em 2018[4]. O Brasil assumiu o

---

1 Sobre o assunto ver BAKER, Philip. Double Taxation Agreements and intemational tax law: a manual on the OCDE model double taxation convention 1977. Londres: 1991. CALIENDO, Paulo. Estabelecimentos permanentes em direito tributário internacional. SP: RT, 2005. GARBARINO, Cario. Manuale di tassazione Intemazionale, Milano: IPSOA, 2006. ROCHA, Sergio André. Transparência Fiscal Internacional no Direito Tributário Brasileiro. Revista Dialética de Direito Tributário, São Paulo, v. 99, p. 112-121, 2003. ROCHA, Sergio André. Troca Internacional de Informações para Fins Fiscais. 1. ed. São Paulo: Quartier Latin, 2015. v. 1 *et* TORRES, Heleno. Pluritributacão internacional sobre as rendas de empresas. São Paulo: Editora Revista dos Tribunais, 2001.

2 A PWC realizou um extenso relaório da implementação das normas internacionais de transparência fiscal no relatório "Tax transparency and country by country reporting - BEPS and beyond". Disponível *in* < http://www.pwc.com/gx/en/services/tax/publications/tax-transparency-and-country-by-country-reporting.html>; acesso em 20.08.2017, às 20:05h.

3 Anguilla, Argentina, Belgium, Bermuda, British Virgin Islands, Bulgaria, Cayman Islands, Colombia, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Faroe Islands, Finland, France, Germany, Gibraltar, Greece, Greenland, Guernsey, Hungary, Iceland, India, Ireland, Isle of Man, Italy, Jersey, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mexico, Montserrat, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Seychelles, Slovak Republic, Slovenia, South Africa, Spain, Sweden, Turks and Caicos Islands, United Kingdom

4 Andorra, Antigua and Barbuda, Aruba, Australia, Austria, The Bahamas, Bahrain, Barbados, Belize, Brazil, Brunei Darussalam, Canada, Chile, China, Cook Islands, Costa Rica, Curaçao, Dominica, Ghana, Grenada, Hong Kong (China), Indonesia, Israel, Japan, Kuwait, Lebanon, Marshall Islands, Macao (China), Malaysia, Mauritius, Monaco, Nauru,

compromisso em participar com a troca automática a partir de 2018. Nesse sentido, saber os limites, conceitos e consequências dessas medidas é algo da maior magnitude.

O Estados Unidos da América estão perseguindo o seu próprio Sistema de troca automática de informações, sob a égide do Foreign Account Tax Compliance Act (FATCA), estabelecido a partir de 2015. Para tanto, foram firmados diversos acordos intergovernamentais (*intergovernmental agréments* - IGAs), visando a troca recíproca e automática de informações entre as jurisdições envolvidas.

A AEOI possui um desenvolvimento histórico de aproximadamente vinte anos e seus fundamentos remontam às cláusulas para a troca de informações, presentes nas convenções internacionais para evitar a dupla tributação da renda, conforme o modelo OCDE.

A partir de 1997, a OCDE passa a indicar *Standard Magnetic Format* (SMF), como solução para a troca automática de informações. A primeira troca multinacional de informações ocorre no âmbito do programa da União Europeia, na diretiva de 2003 sobre os depósitos (*EU Savings Directive*). Outro momento importante será a adoção pelos EUA do modelo FATCA, a partir de 2010, como resposta à crise financeira global.

A principal mudança ocorrerá em 2013 com a adoção formal, pela OCDE, de um projeto de troca automática de informações. A partir desse momento, diversas medidas foram implementadas, tais como: a adoção prematura do modelo, a criação do Global Forum e o compromisso de dezenas de jurisdições na adoção da troca automática.

O AIEA se distingue Modelo Convenção de Troca de Informações Tributárias (TIEA), da OCDE. Este modelo não pressupõe e não autoriza a troca automática de informações fiscais, entre os estados-membros.

A OCDE passou a tratar do assunto como uma de suas prioridades ao considerar a evasão fiscal internacional como um dos mais importantes problemas da globalização. Esta destrói as finanças nacionais, acarreta a desigualdade de tratamento entre os contribuintes,

---

New Zealand, Niue, Pakistan, Panama, Qatar, Russia, Saint Kitts and Nevis, Samoa, Saint Lucia, Saint Vincent and the Grenadines, Saudi Arabia, Singapore, Sint Maarten, Switzerland, Trinidad and Tobago, Turkey, United Arab Emirates, Uruguay, Vanuatu

implica em desvios concorrenciais, oculta dinheiro ilícito e desorganiza as trocas internacionais[5].

A globalização aumenta as possibilidades de investimentos em instituições financeiras internacionais, de maneira exponencial. O que era limitado a apenas algumas instituições ou pessoas, agora se multiplica de modo expressivo. A quantidade de dinheiro canalizada para essas instituições é gigantesca e não se limita a grandes empresas ou a países desenvolvidos. O problema tornou-se muito sério para passar desapercebido pelo conjunto dos governos e a sua solução não pode ser meramente nacional. Somente uma ação coordenada, entende a OCDE, será capaz de reverter esse movimento inexorável dos recursos aos "*portos seguros*" dos investimentos no exterior.

As informações reportadas são das mais variadas ordens, incluindo: juros, dividendos e outros tipos similares de renda, bem como outras situações em que se presuma que o contribuinte esteja escondendo o capital. As pessoas abrangias serão todas as pessoas físicas e jurídicas, mas, especialmente, as "*shell companies*", "*trusts*" e outros arranjos similares, bem como outras entidades tributáveis, mesmo que despersonalizadas.

Terão o dever de reportar atividades todas as instituições financeiras, inclusive as corretoras, veículos coletivos de investimento e as empresas seguradoras. Estas deverão responder a procedimentos sólidos de investigação e fiscalização (*due diligence procedures*).

A troca de informações no ordenamento jurídico nacional

O Brasil ratificou o texto da Convenção sobre Assistência Mútua Administrativa em Matéria Tributária emendada pelo Protocolo de 1º de junho de 2010, firmada pela República Federativa do Brasil em Cannes, em 3 de novembro de 2011, por meio do Decreto nº 8.842, de 29 de agosto de 2016. Esta entrou em vigor no plano externo em 1º de outubro de 2016.

O Brasil procedeu algumas reservas ao texto estabelecido, especialmente ao limitar os tributos e créditos tributários submetidos à

[5] Disponível *in* < http://www.oecd.org/ctp/exchange-of-tax-information/taxtransparency_G8report.pdf>; acesso em20.08.2017, às 19:00h.

autoridade da convenção. Praticamente todos os créditos e tributos serão objeto de assistência para recuperação e notificação. São abrangidos pelo acordo o Imposto sobre a Renda e Contribuição Social sobre o Lucro Líquido; o Imposto sobre os Produtos Industrializados e qualquer outro tributo administrado pela Secretaria da Receita Federal do Brasil.

A autoridade competente, para a República Federativa do Brasil é o Secretário da Receita Federal do Brasil.

Os objetivos da Convenção sobre Assistência Mútua Administrativa em Matéria Tributária estão claramente expressos no seu preâmbulo:

> "Os Estados Membros do Conselho da Europa e os países membros da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), signatários da presente Convenção;
> Considerando que o desenvolvimento dos movimentos internacionais de pessoas, de capitais, de bens e de serviços – conquanto largamente benéfico em si mesmo – veio aumentar as possibilidades de elisão e evasão fiscal, exigindo assim uma cooperação crescente entre as autoridades tributárias;
> Congratulando-se com todos os esforços desenvolvidos ao longo dos últimos anos, em nível internacional, quer a título bilateral quer a título multilateral, para combater a evasão e a elisão fiscais;
> Considerando a necessidade da coordenação de esforços entre os Estados no sentido de incentivar todas as formas de assistência administrativa em matéria de tributos de qualquer espécie, assegurando ao mesmo tempo a proteção adequada dos direitos dos contribuintes;
> Reconhecendo que a cooperação internacional pode desempenhar um papel importante, na medida em que facilita a correta determinação das obrigações tributárias e contribui para que os direitos do contribuinte sejam respeitados;
> Considerando que os princípios fundamentais, em virtude dos quais toda e qualquer pessoa tem direito ao procedimento legal adequado com vista à determinação dos seus direitos e obrigações, devem ser reconhecidos em todos os Estados como sendo aplicáveis em matéria tributária, e que os Estados deveriam esforçar-se no sentido de proteger os legítimos interesses dos contribuintes, inclusive quanto à proteção adequada contra a discriminação e a dupla tributação;
> Convencidos, pois, de que os Estados devem tomar medidas ou prestar informações, tendo em conta a necessidade de proteger o sigilo das informações, e bem assim os instrumentos internacionais relativos à proteção da privacidade e ao fluxo de dados de caráter pessoal;

> Considerando que surgiu um novo ambiente de cooperação e que é desejável dispor de um instrumento multilateral que permita que o maior número de Estados se beneficie do novo ambiente de cooperação e, ao mesmo tempo, implemente os padrões internacionais mais elevados de cooperação no campo tributário;"

As medidas de assistência abrangem tanto as medidas tomadas por órgão judiciais, quanto a assistência administrativa, mediante troca de informações em fiscalizações tributárias simultâneas e a participação em fiscalizações tributárias levadas a efeito no estrangeiro; a cobrança de créditos tributários, incluindo as medidas cautelares e a notificação de documentos.

Serão tributos visados pelo acordo:

i) tributos sobre a renda, os lucros ou os ganhos de capital, ou sobre o patrimônio, estabelecidos por conta das subdivisões políticas ou autoridades locais de uma Parte,
ii) contribuições obrigatórias para a seguridade social pagáveis às administrações públicas ou aos organismos de seguridade social de direito público, e
iii) tributos de outras categorias, com exceção dos direitos aduaneiros, estabelecidos por conta de uma Parte, designadamente:
A) tributos sobre sucessões ou doações,
B) tributos sobre a propriedade imobiliária,
C) tributos sobre o consumo em geral, tais como tributos sobre o valor agregado ou sobre vendas,
D) tributos específicos sobre determinados bens e serviços, tais como aqueles sobre consumos específicos (excise taxes),
E) tributos sobre a utilização ou a propriedade de veículos a motor,
F) tributos sobre a utilização ou a propriedade de bens móveis, com exceção dos veículos a motor,

A troca de informações poderá ser a pedido ou automática. A pedido do Estado requerente, o Estado requerido fornecer-lhe-á todas as informações visadas, relativas a uma pessoa ou a uma transação determinada. Se as informações enviadas não forem suficientes, o Estado requerido deverá tomar todas as medidas para fornecer ao Estado requerente, as informações solicitadas.

A troca automática será autorizada em determinadas categorias

de casos e conforme procedimentos estabelecidos de comum acordo. Poderá haver a troca espontânea de informações, sem pedido prévio, sempre que ocorram as seguintes circunstâncias:

a primeira Parte mencionada tem razões para presumir que possa haver uma perda de receita tributária na outra Parte;

uma pessoa sujeita a tributação obtém, na primeira Parte mencionada, uma redução ou isenção de tributo suscetível de gerar uma majoração de tributo ou uma sujeição a tributo na outra Parte;

as transações comerciais entre uma pessoa sujeita a tributação em uma Parte e uma pessoa sujeita a tributação na outra Parte são conduzidas através de um ou mais países, de tal modo que daí pode resultar uma diminuição do tributo numa ou na outra Parte ou em ambas;

uma Parte tem razões para presumir que uma redução de tributo possa resultar de transferências fictícias de lucros no seio de grupos de empresas e;

e) na sequência de informações fornecidas a uma Parte por outra Parte, a primeira Parte mencionada pôde recolher informações que se revelam de interesse para a determinação do tributo na outra Parte.

Poderá ocorrer a *fiscalização tributária simultânea* sempre que as partes entenderem que os os casos e procedimentos que devam ser objeto de fiscalização tributária simultânea. Esta será levada a cabo em virtude de um acordo nos termos do qual duas ou mais Partes concordam em fiscalizar simultaneamente, cada uma delas no respectivo território, a situação tributária de uma ou mais pessoas, que se revista de interesse comum ou relacionado, com vista à troca de informações relevantes assim obtidas.

Uma grande novidade no acordo é a autorização para que ocorram "*fiscalizações tributárias no exterior*", nesse caso está prevista a autorização para que representantes da autoridade competente do Estado requerente a presenciarem a parte apropriada da fiscalização tributária no Estado requerido. Autoridades estrangeiras poderiam, nos

termos do acordo, acompanhar a fiscalização pela RFB no país e vice-versa. Este pedido poderá ser negado pelo Estado requerido, conforme seu juízo de oportunidade e conveniência.

Talvez a parte mais significativa e revolucionária do acordo, esteja na possibilidade de "*Assistência à Cobrança de Créditos Tributários*". O texto chega a prever a possibilidade de que o Estado requerido procederá à cobrança dos créditos tributários do primeiro Estado mencionado como se se tratasse dos seus próprios créditos tributários. Trata-se de um fato absolutamente inovador, dado que nenhuma legislação anterior havia previsto essa possibilidade.

Outra inovação significativa está na possibilidade do Estado requerido tomar medidas cautelares com vista à cobrança de um montante de tributo, ainda que o crédito seja impugnado ou o título executivo ainda não tenha sido emitido.

Uma questão relevante é a ausência de privilégios. O crédito tributário para cuja cobrança é prestada assistência não se beneficiará, no Estado requerido, de nenhum dos privilégios especialmente conexos com os créditos tributários desse Estado, ainda que o processo de cobrança utilizado seja o mesmo aplicável aos seus próprios créditos tributários.

O art. 18 estabelece quais são as informações objeto do acordo:

> 1. Um pedido de assistência indicará, quando for o caso:
> a) a autoridade ou agência que originou o pedido formulado pela autoridade competente;
> b) o nome, endereço ou quaisquer outros elementos que possibilitem a identificação da pessoa relativamente à qual o pedido é formulado;
> c) no caso de um pedido de informação, a forma como o Estado requerente deseja receber a informação de modo a satisfazer às suas necessidades;
> d) no caso de um pedido de assistência para fins de cobrança ou de medidas cautelares, a natureza do crédito tributário, os elementos constitutivos do crédito e os bens sobre os quais a cobrança pode ser efetuada;
> e) no caso de um pedido de notificação de documentos, a natureza e o objeto do documento a notificar;
> f) se o pedido é conforme com a legislação e a prática administrativa do Estado requerente e se se justifica face às exigências do Artigo 21, parágrafo 2º, alínea g).

São limites ao cumprimento do acordo os direitos fundamentais dos contribuintes, denominados de direitos e salvaguardas. Não poderão ser objeto de pedido:

tomar medidas em desacordo com sua legislação ou sua prática administrativa, ou com a legislação ou a prática administrativa do Estado requerente;

tomar medidas que sejam contrárias à ordem pública;

fornecer informações que não possam ser obtidas com base na sua própria legislação ou prática administrativa, ou na legislação ou prática administrativa do Estado requerente;

fornecer informações suscetíveis de revelar um segredo comercial, industrial, profissional ou um processo comercial, ou informações cuja divulgação seja contrária à ordem pública;

prestar assistência administrativa, se e na medida em que se considere que a tributação do Estado requerente é contrária aos princípios tributários geralmente aceitos, ou às disposições de uma convenção destinada a evitar a dupla tributação ou de qualquer outra convenção celebrada com o Estado requerente;

prestar assistência administrativa tendo em vista a implementação ou o cumprimento de uma disposição da legislação tributária do Estado requerente, ou a satisfação de uma obrigação conexa, que seja discriminatória face a um nacional do Estado requerido em confronto com um nacional do Estado requerente em idênticas circunstâncias;

prestar assistência administrativa, se o Estado requerente não tiver esgotado todas as medidas razoáveis previstas pela sua legislação ou prática administrativa, salvo se o recurso a tais medidas causar dificuldades desproporcionais e;

h) prestar assistência à cobrança nos casos em que os encargos

administrativos para esse Estado sejam claramente desproporcionais face aos benefícios que possam ser obtidos pelo Estado requerente.

O art. 22 da Convenção estabelece os casos de proteção do Sigilo. Serão protegidas quaisquer informações obtidas por uma Parte nos termos da presente Convenção serão consideradas sigilosas e protegidas do mesmo modo que as informações obtidas com base na legislação interna dessa Parte e, na medida necessária para garantir o nível necessário de proteção de dados de caráter pessoal, em conformidade com as salvaguardas exigidas por força da legislação interna da Parte que presta as informações e por ela especificadas.

As informações somente poderão ser utilizadas pelas autoridades competentes nos termos exclusos para os fins mencionados.

O acordo estabelece ainda que as medidas judiciais deverão ser tomadas, tão somente, nos órgãos judiciais nacionais competentes, do Estado requerido.

Considerações Finais

A transparência fiscal prenuncia-se como um dos pilares da fiscalidade no século XXI. A afirmação da isonomia fiscal não pode implicar em ofensa aos direitos do contribuinte. Apesar de cada vez mais tem sido questionada a legitimidade da manutenção do sigilo fiscal, este tem sido consagrado como um verdadeiro direito do contribuinte, tanto pelas convenções internacionais, quanto pela legislação nacional. Esse direito não justifica a fraude ou abuso, nem o direito de ocultar os rendimentos em países com tributação favorecida ou aplicados em empresas estrangeiras *off-shore.* O delicado equilíbrio entre a transparência fiscal e o direito dos contribuintes é um dos grandes desafios do século XXI.

Referências Bibliográficas

BAKER, Philip. Double Taxation Agreements and intemational tax law: a manual on the OCDE model double taxation canvention 1977. Londres: 1991.

CALIENDO, Paulo. Estabelecimentos permanentes em direito tributário internacional. SP: RT, 2005.

GARBARINO, Cario. Manuale di Tassazione Intemazionale, Milano: IPSOA, 2006.

GRUPENMACHER. Betina Treiger. Tratados internacionais em matéria tributária e ordem interna. São Paulo: Dialética, 1999.

MALHERBE; Jacques. Cours de Droit Fiscal International Comparé. Bruxelas: 1972.

PIRES, Manuel. Da dupla tributação jurídica internacional sobre o rendimento. Lisboa Centro de Estudos Fiscais 1987.

ROCHA, Sergio André. Transparência Fiscal Internacional no Direito Tributário Brasileiro. Revista Dialética de Direito Tributário , São Paulo, v. 99, p. 112-121, 2003.

ROCHA, Sergio André. Troca Internacional de Informações para Fins Fiscais. 1. ed. São Paulo: Quartier Latin, 2015. v. 1.

TORRES, Heleno. Pluritributacão internacional sobre as rendas de empresas. São Paulo: Editora Revista dos Tribunais, 2001.

XAVIER, Alberto. Direito tributário internacional do Brasil. Rio de Janeiro; Forense, 2005.

DERECHO, TECNICA E INNOVACIÓN EN LAS LLAMADAS CIUDADES INTELIGENTES. PRIVACIDAD Y GOBIERNO ABIERTO[1].

José Luis Piñar Mañas [2]

I.- El imprescindible diálogo entre derecho y técnica. Lo disruptivo y el derecho. El derecho de acceso a Internet. II.- Ciudades inteligentes. III.- Gobierno abierto como requisito para las ciudades inteligentes. IV.- Privacidad en las ciudades inteligentes. V.-A modo de conclusión.

I.- El imprescindible diálogo entre derecho y técnica. Lo disruptivo y el derecho. El derecho de acceso a Internet.

De un tiempo a esta parte estamos siendo invadidos un día sí y otro también por términos ingleses que expresan lo que en principio parecería ser la última y definitiva novedad técnica y disruptiva que hará que todo cambie definitivamente y ante la cual el derecho no ha sido capaz de reaccionar a tiempo. Ya hace años se habló de las RFID, las *cookies* o más recientemente del *cloud computing*. Hablamos ahora también de *big data, internet of things, wearables, bitcoin, Block Chain, robotics, drones, artificial intelligence, gene drive technology, data driven innovation* y, también, de *Smart cities.*

Sin perjuicio de que no pocos de tales vocablos pueden ser traducidos al español, el escenario parece ser, como digo, inabarcable para un jurista, que se siente abrumado por tantas y tan imprevisibles novedades. Ya hace tiempo que la llamada "Ley de MOORE"[3] ha sido

[1] El presente trabajo se enmarca en el Proyecto de Investigación DER2016-79819-R, del Programa estatal de investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad, del Ministerio de Economía y Competitividad, sobre "Protección de datos, seguridad e innovación: retos en un mundo global tras el Reglamento Europeo de Protección de Datos", del que soy investigador principal. Ha sido ya publicado en el libro dirigido por José Luis PIÑAR MAÑAS y coordinado por Magdalena SUAREZ OJEDA, *Smart Cities: derecho y técnica para una ciudad más habitable*, Editorial Reus, Madrid, 2017.

[2] Catedrático de Derecho Administrativo.

[3] El coste económico de los avances tecnológicos y de nuevos dispositivos es cada vez menor, lo que facilita aún más su uso e implantación. Gordon MOORE expuso hace ya años su visión del futuro de las tecnologías en un breve artículo, de apenas cuatro páginas,

superada por la realidad del avance tecnológico, que trae consigo incuestionables beneficios para la sociedad y el ser humano pero al mismo tiempo implica indudables riesgos para los derechos fundamentales y en particular para la protección de datos personales[4].

Como luego veremos el jurista siempre ha debido enfrentarse a situaciones radicalmente nuevas o diferentes respecto a las anteriores, pero lo cierto es que hoy los acontecimientos a los que se enfrenta no provienen de los avances sociales y culturales, sino fundamentalmente de los de la tecnología. De modo que si siempre ha sido necesario que el derecho esté en constante diálogo con otras realidades o ciencias, hoy resulta imprescindible el diálogo con la técnica.

En otro lugar y ya hace tiempo he señalado que el debate de la relación entre derecho y técnica no es nuevo[5], pero que tiene ahora (o debe tener) características diferentes, pues se ha llegado a cuestionar la posición de regulador o regulado, tanto del derecho como de la técnica.

¿Quién regula a quién? ¿Quién es el regulador y quién el regulado? ¿Está la técnica al servicio del derecho o éste al servicio de aquélla? ¿No estamos ante una situación en la que la técnica está marcando el rumbo del derecho de modo que es éste el que se adapta a la técnica, y en consecuencia incluso el contenido de la idea de justicia queda condicionado por los avances de la técnica? El jurista Natalino IRTI y el filósofo Emanuele SEVERINO debatieron hace años acerca de esa

publicado en 1965, en términos que más adelante se conocerían (y así se conocen hoy) como la "Ley de Moore". Avanzó entonces que "The complexity for minimum component costs has increased at a rate of roughly a factor of two per year ..... Certainly over the short term this rate can be expected to continue, if not to increase. Over the longer term, the rate of increase is a bit more uncertain, although there is no reason to believe it will not remain nearly constant for at least 10 years": "Cramming more components onto integrated circuits", *Electronics*, Volumen 38, Número 8, 19 de Abril de 1965.

4 Vid. PIÑAR MAÑAS, *¿Existe la privacidad?,* Ediciones CEU, Madrid, 2008. CASTELLS, Manuel, *La era de la información. Vol. 1, La sociedad red*, Alianza Editorial, Madrid, 3ª ed., 2005, pág. 70.

5 Al que entre nosotros ha prestado una especial atención ESTEVE PARDO *Técnica, riesgo y Derecho. Tratamiento del riesgo tecnológico en el Derecho ambiental*, Ariel Derecho, Barcelona, 1999, págs. 13 y ss. Y sobre todo su muy sugerente libro *El desconcierto del Leviatán. Política y derecho antes las incertidumbres de la ciencia*, Pons, Madrid, 2009.

relación, ese "diálogo" entre Derecho y Técnica[6]. IRTI considera que el Derecho "si pone sempre come principio ordinatore rispetto alla materia regolata"[7]. SEVERINO, sin embargo, concluye tajante que "la tecnica è destinata a diventare la regola e tutto il resto il regolato"[8]. Como ha señalado Lorenzo MARTIN RETORTILLO, "la técnica no tiene porqué arrumbar al Derecho"[9], pero este deseo no siempre se cumple. ESTEVE PARDO ha llegado a decir incluso que "se está estableciendo como una nueva división de poderes entre el poder establecido por la ciencia y el poder establecido por el derecho", de modo que "la ciencia está ocupando extensos territorios tradicionalmente atribuidos al derecho y efectivamente dominados por él hasta tiempos muy recientes"[10]. RODOTA, en su magnífico libro *La vita e le régole. Tra Diritto e non Diritto*[11], que ha sido traducido al español[12], se refiere a menudo a los límites que debe haber entre el derecho y la técnica, y en otras ocasiones ha llamado la atención certeramente acerca de la influencia de las nuevas tecnologías en la democracia[13].

En cualquier caso no es ésta la primera vez, ni será la última, que el Derecho se enfrenta a situaciones disruptivas. GARCIA DE ENTERRIA, por ejemplo, ya expuso magistralmente hace años cómo la Revolución Francesa "fue un tajo decisivo entre lo que a partir de entonces se llamaría, muy justamente, el Antiguo Régimen y el nuevo orden político y social que pretendió crearse sobre fundamentos enteramente

---

6 *Dialogo su Diritto e Técnica*, Editori Laterza, Roma-Bari, 2001. A este debate me he referido ya en "Revolución tecnológica…", op. cit., págs. 56 y ss.

7 Op. cit., pág. 15.

8 Op. cit., pág. 80.

9 "Presentación", op. cit., pág. 10.

10 *El desconcierto del Leviatán…., op. cit.,* págs. 99 y 100.

11 Feltrinelli, Milano, 2006. Hay una segunda edición, ampliada, con la adición de un uevo capítulo, en Universale Economica Feltrinelli, Milano, 2009.

12 *La vida y las reglas. Entre derecho y no derecho*, Trotta, Madrid, 2010, con prólogo de José Luis Piñar.

13 Véase *Tecnologie e diritti*, Il Mulino, Bari, 1995. *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Editori Laterza, Roma-Bari, 1997. Hay traducción al español: *Tecnopolítica. La democracia y las nuevas tecnologías de la información*, Losada, Buenos Aires, 2000.

nuevos"[14]. Todo cambió a partir de entonces, y el Derecho hubo de adaptarse a ello. Con la Revolución Francesa "toda la representación del mundo social y colectivo cambió súbitamente. La vieja y rígida estructura social fue rasgada de un sólo golpe"[15]. Y así como ahora hemos de acostumbrarnos a marchas forzadas a un nuevo lenguaje dictado desde la técnica, también entonces surgió un nuevo léxico, pero desde la sociedad y el derecho: "la Revolución fue... desde sus orígenes... una guerra de palabras"[16]. Surge así un nuevo lenguaje jurídico, la "lengua de los derechos", explicada "no como una simple aparición de nuevos términos, en un plano estrictamente técnico de análisis léxico o sintáctico, sino como la expresión de un nuevo discurso jurídico que ofrece un nuevo modelo de relación entre los hombres"[17].

Por tanto, no supone ninguna novedad que el derecho deba hacer frente a cambios radicales en la sociedad. Más bien al contrario. En un escenario, además, presidido por un nuevo lenguaje anglosajón que se impone desde el mundo tecnológico y que no siempre encierra novedades realmente disruptivas.

En cualquier caso, los juristas estamos casi obligados a convivir con la técnica y a hacer frente a los retos que plantea, que como digo supone indudables avances para la sociedad, pero que al mismo tiempo implica no pocas amenazas para los derechos, en particular para la privacidad o la protección de datos de carácter personal. Al mismo tiempo implica la necesidad de configurar nuevos derechos, los de los llamados ciudadanos digitales, que buscan reconocer los nuevos derechos que esta nueva situación trae consigo y entre los que se encuentra, por ejemplo, el propio derecho de acceso a internet[18], incluso derecho de acceso a alta velocidad o a través de banda ancha. Son muchos los motivos que exigen el reconocimiento de esos nuevos derechos; de entre ellos ahora me interesa resaltar el hecho de que el

---

[14] *La lengua de los derechos. La formación del Derecho Público Europeo tras la Revolución Francesa*, Alianza Universidad, Madrid, 1994, pág. 18.

[15] Op. cit. pág. 26.

[16] Op. cit, pág. 27.

[17] Op. cit., pág. 37.

[18] RODOTÀ se ha referido a la "ciudadanía digital" en *Il mondo nella rete. Quali i diritti, quali i vincoli*, Editori Laterza, Roma, 2014, págs. 13 y ss.

acceso a internet en condiciones de igualdad va a ser en breve requisito para poder desarrollar una vida normal de acuerdo a los nuevos estándares que la tecnología va a ir imponiendo. No sólo debe garantizarse el acceso a internet para a su vez garantizar el acceso a la cultura, el derecho a la libertad de información o el derecho a la participación democrática. Algunas consecuencias del uso de internet, como el uso masivo de datos y la generación de información que ello implica *(big data, data driven innovation*), y algunos desarrollos de la red, como la internet de las cosas (*internet of things*), van a cambiar radicalmente la vida en general y la vida en las ciudades en particular. No es aventurado afirmar que en un futuro no muy lejano la vida cotidiana de gran parte de la población (no la de unos pocos) va a estar condicionada por el uso de internet. Desde el uso del transporte público a la de los servicios de salud; desde la compra de entradas para espectáculos a la entera relación con la Administración Pública; desde el uso de vehículos sin conductor a la reserva de plazas en los aparcamientos; desde el conocimiento del estado del tráfico a la facturación de cualquier servicio o prestación; desde la compra de cualquier producto, por pequeño o sofisticado que sea, al pago de cualquier bien, producto o servicio o la relación con los bancos; desde la monitorización constante de nuestra salud a la atención médica a distancia. Se habla ya del "hombre aumentado": en la presentación del Informe de la Fundación Telefónica *La Sociedad de la Información en España 2016*[19] se afirma que "Las *wearables*, la tecnología vestible evoluciona y se acerca hasta la propia piel del usuario para pasar a ser una parte de nosotros. Sí, los dispositivos y las personas se integran, lo que supone en muchos casos aumentar las capacidades humanas por medio de la tecnología. Exoesqueletos, elementos biónicos, dispositivos en la piel, incluso, bajo la piel (*biohacking*) o en otros puntos del organismo: la idea de un "hombre aumentado" ya es un hecho"[20]. Algo que exige al jurista estar especialmente atento por las implicaciones que pueda tener en el ámbito de la propia dignidad de la persona, de su posible cosificación.

---

19 https://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/558/

20 https://www.fundaciontelefonica.com/2017/02/24/sie-2016-tendencias-internet/

La práctica totalidad de las manifestaciones de la vida cotidiana van a estar directa o indirectamente vinculadas a internet. Y es importante resaltar que me refiero a la vida cotidiana, a la normal y corriente, a la del "uomo qualunque", no a la de una minoría privilegiada con acceso también privilegiado a las tecnologías de la información y el conocimiento. Esa vida cotidiana es también la que va a desarrollarse en la ciudad, que dentro de poco será también impensable sin internet. Y es precisamente en este escenario en el que el derecho de acceso a internet cobra especial relevancia. Pues el desarrollo de las ciudades inteligentes, con todo lo que ello implica para el ser humano, requiere ineludiblemente de Internet. Tanto para su puesta en funcionamiento por parte de las instituciones públicas y privadas implicadas, como para aprovechar todo lo que aportan a las personas en general.

En consecuencia, no es posible pensar siquiera en las *Smart Cities* sin Internet y por tanto su desarrollo y consolidación, como modelo normal de la ciudad del próximo futuro, requieren reconocer el derecho de acceso a Internet como derecho fundamental, no sólo vinculado al derecho a la libertad de información y expresión. Ya el Informe del Relator Especial de Naciones Unidas, sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, presentado el 16 de mayo de 2011 al Comité de Derechos Humanos de la ONU[21], pone de manifiesto rotundamente que limitar el acceso a internet es limitar el derecho fundamental a la libertad de expresión e información. Por su parte, el Foro de Gobernanza en Internet de Naciones Unidas ha propuesto un listado de diez derechos y principios para Internet entre los que se encuentran el de Accesibilidad (toda persona tiene igual derecho a acceder y utilizar Internet de forma segura y libre) y el de Igualdad (todo el mundo tendrá acceso universal y abierto a los contenidos de Internet, libre de priorizaciones discriminatorias, filtrado o control de tráfico por razones comerciales, políticas o de otro)[22]

Es por tanto necesario dar un paso más hacia la consideración del derecho de acceso a Internet como manifestación del libre desarrollo de la personalidad y del desarrollo de la vida cotidiana. Internet como medio para poder llevar una vida normal en una sociedad medianamente

[21] http://www.acnur.org/t3/fileadmin/Documentos/BDL/2015/10048.pdf?view=1

[22] http://derechoseninternet.org/docs/IRPC_Carta_Derechos_Humanos_Internet.pdf

avanzada y en cualquier caso como medio para dar el paso a una sociedad mejor. Sobre todo a partir de la implantación y desarrollo de la *Internet of things* que supone superar la idea de Internet como medio para la comunicación, intercambio, creación de información y conocimiento, y plantear la idea de Internet como ámbito vital. Hace tiempo apuntaba que los jóvenes ya no viven "con" Internet sino que viven "en" Internet. Lo que para los adultos es una "herramienta" de un alcance e importancia extraordinarios, para ellos es una "forma de vida" que ya es la cotidiana, de modo que ya es "su" forma de vida[23]. Por tanto el derecho de acceso a Internet debe ser considerado como derecho fundamental vinculado no sólo al derecho a la libertad de expresión e información sino también al derecho al libre desarrollo de la personalidad. Algo especialmente relevante si hablamos de ciudades inteligentes, que, sencillamente, no son posibles sin Internet.

Ahora bien, junto a este derecho, que me parece incuestionable, debería también reconocerse el derecho a vivir sin Internet. O lo que es lo mismo, que el derecho de acceso a Internet no se convierta en una obligación o necesidad de vivir con o en Internet. RODOTÀ ha hablado con razón del "derecho a hacer silencioso el chip", el derecho "a desactivar el chip contenido en un *badget* o en cualquier otro dispositivo que la persona lleve consigo o que se encuentre en su auto o en su casa, interrumpiendo de este modo la transmisión de datos a un sujeto determinado"[24]. Lo que se podría extender a la posibilidad de desarrollar una vida cotidiana normal sin Internet. Cierto que la persona que así lo decida deberá ser consciente de las posibilidades que entonces pierde en el ámbito de las relaciones privadas o de mercado por no utilizar la Red. Pero esta opción personal, incluso vital, no debe afectar a las relaciones con lo público en general y con las Administraciones Públicas en particular. Y en este sentido debería reflexionarse acerca de si la obligación que la Ley 39/2015 impone a las personas jurídicas y los

---

[23] PIÑAR MAÑAS, "El Derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales", en el libro también por mi dirigido *Redes sociales y privacidad del menor*, REUS-Fundación Solventia, Madrid, 2011, pág. 62.

[24] A ese derecho se refiere RODOTÀ, en *Il mondo nella rete*…, op. cit, pág. 33. Se trata del derecho "a desactivar el chip contenido en un *badget* o en cualquier otro dispositivo que la persona lleve consigo o que se encuentre en su auto o en su casa, interrumpiendo de este modo la transmisión de datos a un sujeto determinado".

profesionales de relacionarse necesariamente por medios electrónicos con las Administraciones es un avance o puede llegar a ser una traba dado que no todos tienen a su alcance el uso de las tecnologías necesarias para ello y, lo que también es grave, que no pocas Administraciones, sobre todo pequeños municipios, carecen de medios técnicos para permitir ese acceso.

Sin que debamos olvidar que las *Smart cities* no son las únicas ciudades posibles. En ningún caso debe imponerse la dictadura de la ciudad inteligente sólo accesible o sólo pensada para los conectados a Internet. Las tecnologías de la información deben estar al servicio de la persona, no fagocitarla. El ser humano, al menos en su relación con los poderes públicos, debe beneficiarse de la innovación tecnológica aunque él mismo decida permanecer al margen de dicha innovación, en general o en relación con extremos que considere amenazantes para sus derechos, muy en particular su derecho a la privacidad o protección de datos. No debe ser necesario "cosificar" a la persona o convertirlo en una base de datos para que pueda desarrollar sus opciones vitales en la ciudad o fuera de ella.

II.- Ciudades inteligentes.

No es fácil alcanzar una definición conceptual de lo que debe entenderse por *Smart city* o ciudad inteligente. Así lo han recordado Annalisa COCCHIA o Anthony M. TOWNSEND[25]. Ciudad inteligente es aquélla que se vale de la innovación tecnológica para ofrecer un entorno más habitable a las personas. Pero, como he señalado, no puede convertirse en una ciudad exclusiva para los familiarizados con la innovación y excluyente para los que o no lo están o no quieren estarlo. Pues en este caso estaríamos no ante una ciudad inteligente, sino robotizada y deshumanizada. Lo contrario a inteligente y sostenible.

---

[25] "Smart and Digital City: a Systematic Literature Review", en Renata Paola DAMERI y Camille ROSENTHAL-SABROUX (Eds.) *Smart City: How to Create Public and Economic Value with High Technology in Urban Space*, Springer, 2.014, págs. 13 y ss. Vid. también Anthony M. TOWNSEND, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*, Norton & Company, Londres-Nueva York, 2013.

Dicho lo anterior, me basaré en ciertos documentos más o menos conocidos, pero no doctrinales o conceptuales, para describir lo que suele entenderse en la práctica por ciudad inteligente.

El Plan Nacional de Ciudades Inteligentes (Marzo 2015)[26] del Gobierno[27] acoge la definición de ciudad inteligente propuesta por el Grupo Técnico de Normalización 178 de AENOR (AEN/CTN 178/SC2/GT1 N 003):

> "Ciudad inteligente (Smart City) es la visión holística de una ciudad que aplica las TIC para la mejora de la calidad de vida y la accesibilidad de sus habitantes y asegura un desarrollo sostenible económico, social y ambiental en mejora permanente. Una ciudad inteligente permite a los ciudadanos interactuar con ella de forma multidisciplinar y se adapta en tiempo real a sus necesidades, de forma eficiente en calidad y costes, ofreciendo datos abiertos, soluciones y servicios orientados a los ciudadanos como personas, para resolver los efectos del crecimiento de las ciudades, en ámbitos públicos y privados, a través de la integración innovadora de infraestructuras con sistemas de gestión inteligente."

El Plan Nacional de Ciudades Inteligentes forma parte de la Agenda Digital para España, entre cuyos objetivos se encuentran la adopción de medidas para contribuir al desarrollo de las industrias de futuro; potenciar el desarrollo y uso del *cloud computing*; potenciar el desarrollo y uso de técnicas de *big data,* y para potenciar el empleo de las TIC para favorecer el ahorro energético y el desarrollo de ciudades e infraestructuras inteligentes que garanticen su sostenibilidad en el tiempo y contribuyan al desarrollo de nuestra economía. En relación con estas últimas se incluyen las siguientes:

---

[26] http://www.minetad.gob.es/turismo/es-ES/Novedades/Documents/Plan_Nacional_de_Ciudades_Inteligentes.pdf

[27] Elaborado por el entonces Ministerio de Industria, Energía y Turismo pretende **impulsar en España la industria tecnológica de las Ciudades Inteligentes** y ayudar a las entidades locales en los procesos de transformación hacia Ciudades y Destinos Inteligentes. Forma parte de la Agenda Digital para España (http://www.agendadigital.gob.es/agenda-digital/recursos/Recursos/1.%20Versi%C3%B3n%20definitiva/Agenda_Digital_para_Espana.pdf) .

Participar en el desarrollo de las iniciativas de la UE en materia de *green* TIC, *smart grids* y *smart cities.*

Establecer canales de información y asesoramiento para empresas y ciudadanía que deseen incorporar medidas TIC para el ahorro energético y disminución de emisiones contaminantes.

Definir y establecer un sistema de medición del ahorro energético e impacto medioambiental vinculado a las TIC.

Impulsar el uso de las TIC en infraestructuras para la provisión de servicios básicos, como son las de transporte de agua, electricidad y energía.

Diseñar un Plan que unifique criterios, principios y despliegues de redes inteligentes y ciudades inteligentes

Definir estándares que faciliten la reutilización de la información generada en el ámbito de las *smart cities* para el desarrollo de nuevos servicios.

La Agenda Digital prevé incluso la creación de un Comité de Normalización de Ciudades Inteligentes, creado ya en el seno de AENOR[28]

El Plan Nacional de Ciudades Inteligentes, que contempla la creación de un Consejo Asesor de Ciudades Inteligentes[29], se estructura en torno a cuatro ejes[30]:

> I: Facilitar a las ciudades el proceso de transformación hacia una Ciudad Inteligente. Tiene como objetivo impulsar la demanda facilitando a los municipios el proceso de transformación en Ciudades Inteligentes mediante ayudas al desarrollo y especialización de las mismas. Se

[28] http://www.smartcities.es/2013/03/06/el-comite-tecnico-de-normalizacion-sobre-ciudades-inteligentes-de-espana-sigue-avanzando/

[29] En él estarán presentes, entre otros: SETSI, Red.es, SEGITTUR, IDAE, EOI, las entidades locales y los representantes de la industria. Este órgano asesor y consultivo, adscrito al MINETUR, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, tendrá como misión emitir informes, proponer estrategias, contribuir a conformar la posición española en foros internacionales, coordinar esfuerzos y favorecer la participación de administraciones, empresas, expertos e industria: pág. 8 del Plan.

[30] http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-nacional-ciudades-inteligentes.aspx

> promoverá la estandarización, la interoperabilidad, la reutilización y el seguimiento de las iniciativas más relevantes. Se elaborará un libro blanco que permita avanzar en la métrica y la gobernanza de Ciudades y Destinos Turísticos Inteligentes.
> II: Proyectos demostradores de la eficiencia de las Tecnologías de la Información y de las Comunicaciones en la reducción de costes, mejoras en la satisfacción ciudadana y creación de nuevos modelos de negocio. Facilitará el desarrollo de proyectos que demuestren la eficiencia de las TIC en la reducción de costes, las mejoras en la satisfacción ciudadana y la creación de nuevos modelos de negocio, mediante ayudas financieras, medidas de apoyo y financiación a iniciativas de cooperación público-privada y la promoción de la compra pública innovadora.
> III: Desarrollo y crecimiento de la industria TIC. Se orienta al desarrollo y crecimiento de la industria TIC, con actuaciones que impulsen nuevas soluciones tecnológicas que contribuyan al avance de las Ciudades Inteligentes y fomenten su internacionalización.
> IV: Comunicación y difusión del Plan Nacional de Ciudades Inteligentes. Orientado a la comunicación y difusión del Plan, para asegurar su comprensión, orientar el desarrollo de las ciudades inteligentes mediante procesos participativos y comunicar la oportunidad de orientar el proceso de construcción de las nuevas ciudades desde soluciones abiertas, interoperables y reutilizables.

Creo que no es superfluo contar con la descripción que acabo de hacer de lo que se entiende por ciudades inteligentes y la que parece decidida intención de los poderes públicos de impulsarlas. Algo que es ya una tónica general a nivel mundial. Incluso hay en marcha proyectos de *Smart Nations* como es el caso de Singapur[31], basado en cinco objetivos iniciales: transporte, vivienda y medio ambiente, productividad de las empresas, salud y tercera edad, y servicios públicos.

En lo que ahora nos interesa, las ciudades inteligentes no son viables sin el tratamiento masivo de información, tanto pública como la que afecta a las personas en particular. Lo que se refleja en al menos dos direcciones: por un lado el reto del gobierno abierto y la reutilización de la información pública; por otro el tratamiento de datos personales, con lo que esto implica para la privacidad.

[31] https://www.smartnation.sg

III.- Gobierno abierto como requisito para las ciudades inteligentes.

Una de las "revoluciones" que están produciéndose en no pocos países y por supuesto también en el nuestro es la de la transparencia. Si bien los países nórdicos conocen desde hace siglos la transparencia y el acceso a la información (la primera ley de acceso a la información es seguramente la *Freedom of the Press Act* aprobada en Suecia en 1766, que permitió la publicación de documentos del gobierno y el acceso público a los mismos)[32], en otras latitudes, como ocurre con los países mediterráneos o de tradición jurídica continental, la situación era sin duda muy diferente. Hoy las cosas están cambiando. La transparencia, en sus distintas manifestaciones, está presente en nuestras leyes, como la Ley 19/2013, de transparencia, acceso a la información y buen gobierno y las leyes de las Comunidades Autónomas aprobadas sobre la materia[33].

---

32 A ello me he referido en «Transparencia y derecho de acceso a la información pública. Algunas reflexiones en torno al derecho de acceso en la Ley 19/2013, de transparencia, acceso a la información y buen gobierno». *Revista catalana de dret públic*, Núm. 49 (diciembre 2014), pp. 1-19, y en otras ocasiones anteriores.

33 Ley 4/2011, de 31 de marzo, de la buena administración y del buen gobierno de las Illes Balears.

Ley Foral 11/2012 de la Transparencia y del Gobierno Abierto (modificada por la Ley Foral 5/2016, de 28 de abril).

Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura.

Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.

Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno de Cataluña.

Ley 12/2014, de 26 de diciembre, de transparencia y de acceso a la información pública de Canarias.

Ley 12/2014, de 16 de diciembre, de transparencia y participación ciudadana de la Comunidad Autónoma de la Región de Murcia.

Ley 3/2014, de 11 de septiembre, de Transparencia y Buen Gobierno de La Rioja.

Ley 8/2015, de 25 de marzo, de Transparencia Pública y Participación Ciudadana de Aragón.

Ley 2/2015, de 2 de abril, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana (modificada por Ley 10/2015, de 29 de diciembre y Ley 2/2016, de 4 de marzo).

Ley 3/2015, de 4 de marzo, de transparencia y participación ciudadana de Castilla y León.

Ley 1/2016, de 18 de enero, de transparencia y buen gobierno de Galicia.

Y precisamente una de las expresiones de la transparencia es el llamado gobierno abierto[34], *open government*, o el modelo de datos abiertos, *open data.* Algo que es imprescindible para poder llevar adelante el desarrollo y la implantación de las ciudades inteligentes.

Según la Carta Internacional de Datos Abiertos, "datos abiertos son datos digitales que son puestos a disposición con las características técnicas y jurídicas necesarias para que puedan ser usados, reutilizados y redistribuidos libremente por cualquier persona, en cualquier momento y en cualquier lugar"[35]. Falta una previsión esencial en esa definición, que es el hecho de que ha de referirse a datos en poder, en principio y con carácter general, de organismos públicos. Esta circunstancia es la que conecta el gobierno abierto con la transparencia y el acceso a la información pública. Y la que incide en el desarrollo de las ciudades inteligentes, que sencillamente no serían posibles sin el acceso a determinada información pública. Asimismo es imprescindible resaltar la trascendencia que tiene el régimen de reutilización de dicha información, hoy regulado con carácter general en la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público[36], modificada por la Ley 18/2015, de 9 de julio. Ley que define como datos abiertos a "aquellos que cualquiera es libre de utilizar, reutilizar y redistribuir, con el único límite, en su caso, del requisito de atribución de su fuente o reconocimiento de su autoría". Por documento se entiende "toda información o parte de ella, cualquiera que sea su soporte o forma de expresión, sea esta textual, gráfica, sonora visual o audiovisual, incluyendo los metadatos asociados y los datos contenidos con los niveles más elevados de precisión y desagregación. A estos efectos

---

Asimismo ténganse en cuenta el Proyecto de Ley de Transparencia de Castilla La Mancha, de 6 de septiembre de 2016 y el Proyecto de ley de transparencia, participación ciudadana y buen gobierno del sector público vasco, así como el Anteproyecto de ley del Principado de Asturias de transparencia y buen gobierno, de 2015.

34 Recientemente vid. CERRILLO I MARTÍNEZ, Agustí, "El gobierno abierto", en el libro colectivo coordinado por él mismo *A las puertas de la administración digital: Una guía detallada para la aplicación de las Leyes 39/2015 y 40/2015,* INAP, Madrid, 2016, págs. 143-180

35 http://opendatacharter.net/principles-es/

36 Que traspone la Directiva 2003/98/CE, de 17 de noviembre de 2003, del Parlamento Europeo y del Consejo, relativa a la reutilización de la información del sector público.

no se considerarán documentos los programas informáticos que estén protegidos por la legislación específica aplicable a los mismos". En cualquier caso, los datos o documentos han de ser "elaborados o custodiados por las Administraciones y organismos del sector público", según reza el artículo 1 de la Ley 37/2007[37]. Pero de nada serviría diseñar un modelo de gobierno abierto y reutilización de la información pública si no se garantiza, o al menos regula, la interoperabilidad de los datos e informaciones. Tal es el objeto del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica[38].

La transparencia y el gobierno abierto no tienen, sin embargo, gran tradición entre nosotros. De hecho España entró a formar parte de la Alianza para el Gobierno Abierto[39] sólo en abril de 2011. Pieza esencial de la Alianza son los Planes de Acción de Gobierno Abierto. El 1º Plan de Acción[40] fue presentado en la I Conferencia Internacional de la Alianza, celebrada en Brasil en abril de 2012. A mediados del año 2014 España presentó su II Plan de Acción (2014-2016)[41], que no hace referencia a las ciudades ni a las *smart cities*. No obstante, en el Informe de Autoevaluación del II Plan de Acción[42] se incluye un Compromiso, el 5º, sobre "Acceso a la información geográfica y posibilidad de reutilización de la misma", en el que se señala: "La política de apertura de datos

---

37 Por cierto, en un anexo de definiciones la Ley contiene una peculiar e innecesaria definición de Universidad: "Todo organismo del sector público que imparta enseñanza superior post-secundaria conducente a la obtención de títulos académicos".

38 Sobre la interoperabilidad vid entre otros MARTÍNEZ GUTIÉRREZ, Rubén, "Cooperación y coordinación entre Administraciones públicas para el impulso de la administración electrónica. La interoperabilidad", en PIÑAR MAÑAS, (dir.): *Administración electrónica y ciudadanos*, Civitas-Thomson-Reuters, Cizur Menor (Navarra), 2011, págs. 667 y ss.

39 *Open Government Partneship -OGP-*. https://www.opengovpartnership.org/

40 http://transparencia.gob.es/transparencia/transparencia_Home/index/GobiernoParticipacion/Gobierno-abierto/I-PlanAccionGA.html

41 http://transparencia.gob.es/transparencia/transparencia_Home/index/GobiernoParticipacion/Gobierno-abierto/II-PlanAccionGA.html

42 http://transparencia.gob.es/transparencia/dam/jcr:35be333d-5e3d-4f9c-9e3f-1b177f87c3ba/gobierno-abierto-OGP-autoevaluacion-anexos-II-plan-nacional.pdf

abiertos produce los siguientes resultados directos: Mejora en la coordinación entre las diferentes administraciones públicas a todos los niveles. La compartición de información geográfica temática y de referencia utilizando estándares abiertos facilita la comunicación y el intercambio entre organizaciones y permite el desarrollo de proyectos de interés común como las Smart cities". En estos momentos está elaborándose el III Plan de Gobierno Abierto para el periodo 2017-2019[43]. En mayo de 2017 se ha hecho público el Borrador del Plan[44] y ha de decirse que en el mismo no hay referencia alguna a las ciudades inteligentes.

IV.- Privacidad en las ciudades inteligentes

La implantación y desarrollo de las ciudades inteligentes requiere tratar ingentes cantidades de información y datos personales. Datos que fluyen entre los sectores público y privado y que facilitan el conocimiento y predicción de situaciones que permiten una ciudad más habitable. Asimismo requiere de la interconexión de dispositivos que en el marco de la Internet de las cosas permiten asimismo obtener información de capital interés para lograr ese objetivo.

Esta circunstancia exige tener presente en todo caso el impacto que sobre la protección de datos puede llegar a tener la apuesta por las ciudades inteligentes. El escenario es claro: para conocer y predecir el estado del tráfico, la mejor opción de transporte público en nuestros desplazamientos, el modo de ahorrar energía, la oferta de bienes o de servicios, públicos o privados, o de actividades culturales que se adapten mejor a nuestras preferencias, para advertirnos de cualquier riesgo para nuestra salud y de los centros a los que podemos acudir, para conocer dónde se localiza el vehículo eléctrico más cercano que podemos utilizar para nuestra movilidad, para todo esto y mucho más es necesario tratar datos personales, que en muchas ocasiones implica el acceso a los

43 http://transparencia.gob.es/transparencia/transparencia_Home/index/GobiernoParticipacion/Gobierno-abierto/IIIPlan.html

44 http://transparencia.gob.es/transparencia/dam/jcr:d9b52138-6e25-4f47-9de2-ec253ff23a63/2017_Borrador_III_PLAN_Gobierno_Abierto.pdf

mismos por parte de terceros que no siempre somos capaces de identificar correctamente.

Lo anterior implica que no es posible plantear la cuestión de las ciudades inteligentes sin tener presente el régimen de la protección de datos de carácter personal. No se trata ahora de identificar qué tratamientos de datos han de llevarse a cabo y quién lo hace; tampoco de determinar quién puede tener la consideración de responsable o encargado del tratamiento. Sino de ser conscientes de que el respeto al derecho a la protección de datos es imprescindible para un desarrollo lícito de las ciudades inteligentes.

Esta consideración tiene especial trascendencia si tenemos en cuenta que tal derecho consiste esencialmente en la atribución a las personas de un poder de disposición sobre sus propios datos. Lo que se traduce en los principios que definen el derecho y que se recogen en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que trae causa de la Directiva 95/46/CE, de la que es trasposición, y que hoy han sido ampliados en el 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[45].

El artículo 5º del Reglamento recoge precisamente los principios relativos al tratamiento: Licitud, lealtad, transparencia; limitación de finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad; responsabilidad proactiva; y licitud del tratamiento[46]. Pero además el artículo 25 pone especial énfasis en dos principios de especial importancia en el desarrollo de las *Smart cities*: privacidad desde el diseño y privacidad por defecto[47].

---

[45] DOUE L 119, de 4 de mayo de 2016.

[46] Sobre la regulación de dichos principios en el Reglamento, vid. PUYOL MONTERO, Javier, "Los principios del Derecho a la Protección de Datos", en PIÑAR MAÑAS (Director), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, REUS, Madrid, 2016, págs. 135 y ss.

[47] Vid. DUASO CALES, Rosario, "Los principios de protección de datos desde el diseño y protección de datos por defecto", en PIÑAR MAÑAS (Director), *Reglamento General de Protección de Datos….. Op. cit.,* págs. 295 y ss.

El Reglamento incorpora alguna novedad en relación con la Directiva y la LOPD. Ésta se refiere a los principios de información (art. 5), consentimiento (arts. 6 y 11), finalidad (art. 4), calidad del dato (art. 4) y seguridad (art. 9). Sin poder entrar ahora en el alcance de los cambios introducidos, lo cierto es que en cualquier caso debe garantizarse el control de los propios datos personales[48] y debe incorporarse la protección de datos al discurso y la agenda de las *Smart cities*. No en vano la Carta de Derechos Fundamentales de la Unión Europea recoge en su artículo 8, en términos muy amplios, el derecho a la protección de datos, derecho que se reconoce a todas las personas y que debe condicionar cualquier tratamiento de datos que se lleve a cabo. Y como hemos señalado antes, si algo caracteriza a las ciudades inteligentes es el masivo uso de datos que llevan a cabo múltiples actores, públicos y privados, y la necesidad de interconectar millones de dispositivos. En definitiva me refiero al *Big Data* y a la Internet de la Cosas, *Internet of things.*

Como señala el llamado Grupo de Trabajo del Artículo 29[49] en su Documento *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU (WP 221)*, de 16 Septiembre de 2014[50], "*Big data*" es un término general que cubre un gran número de operaciones de tratameinto de datos personales, algunas de las cuales están hoy bien identificacadas mientras que otreas habrán de desarrolarse en el future. Añado yo que muchas de esas operaciones se aplican ya al desarrollo de las ciudades inteligentes (control y ordenación del tráfico, gestión y ahorro eficiente y sostenible

---

48 Lo que ha dado pie a hablar del derecho a la autodeterminación informativa. Vid. LUCAS MURILLO DE LA CUEVA, Pablo, y PIÑAR MAÑAS, José Luis, *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009.

49 Dicho Grupo de Trabajo está constituido por las Autoridades de Protección de Datos de los Estados miembros de la Unión Europea y recibe esa denominación por haber sido creado en virtud del artículo 29 de la Directiva 95/46/CE. El nuevo Reglamento Europeo de Protección de Datos transforma en parte su naturaleza y régimen y lo denomina Comité Europeo de Protección de Datos. Véase CERVERA NAVAS, Leonardo, "El Comité Europeo de Protección de Datos", en PIÑAR MAÑAS (Director), *Reglamento General de Protección de Datos….. op. cit.,* págs. 527 y ss.

50 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

de energía, oferta de bienes y/o servicios acordes a las preferencias de las personas, monitorización de las personas por motivos de salud, y tantas otras….) y sin duda otras muchas más se desarrollarán en el futuro. El desarrollo de las tecnologías de *big data* genera sin duda importantes beneficios para las personas y para la sociedad, como señala el Documento del WP29. Pero así mismo puede tener importancias consecuencias sobre la protección de las personas en relación con el tratamiento de sus datos personales. Genera no pocas cuestiones sociales, jurídicas y éticas, y en este marco la legislación europea sobre protección de datos adquiere especial importancia. Los principios de protección de datos a que antes me refería, contenidos en la Directiva 95/46/CE y también en el nuevo Reglamento, adquieren especial relevancia, y muy en particular los de finalidad y calidad, así como el de minimización de los datos, a veces confundido o subsumido en los anteriores. Es más, como sigue el WP29, el cumplimiento de tales principios es un elemento esencial para generar confianza en los usuarios, que son conscientes (aunque no siempre) de que sus datos están siendo tratados con fines de *big data.* Y en este sentido debemos tener en cuenta dos cuestiones más: por un lado la necesidad de no olvidar la posibilidad que siempre ha de darse a las personas de ejercer sus derechos en materia de protección de datos ante los responsables de los tratamientos. Derechos tales como los de acceso, rectificación, cancelación y oposición[51], y también el derecho al olvido[52] y el derecho

[51] Artículos 13 a 19 de la LOPD y artículos 23 a 36 del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre. Sobre la regulación de tales derechos contenida en los artículos 15 y ss. del Reglamento Europeo de Protección de Datos vid. ALVAREZ CARO, María, "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", en PIÑAR MAÑAS (Director), *Reglamento General de Protección de Datos….., op.cit.*, págs. 227 y ss.

[52] La bibliografía sobre el derecho al olvido es ya muy abundante. Vid. recientemente ALVAREZ CARO, María, "El derecho a la supresión o al olvido", en PIÑAR MAÑAS (Director), *Reglamento General de Protección de Datos….., op.cit.*, págs. 241 y ss. Asimismo BERROCAL LAZAROT, Ana, "El derecho de supresión de datos o derecho al olvido en el Reglamento General de Protección de Datos", en *Revista General de Legislación y Jurisprudencia*, III Epoca, nº 1 (enero-marzo) de 2017, págs. 7 y ss. Contiene una descripción muy útil de la situación.

a la portabilidad[53]. Por otro lado, el hecho de que con las técnicas de *big data* los usuarios pueden, en efecto, recibir servicios o información muy relevante para mejorar la calidad de vida en las ciudades. Pero siendo esto así, no podemos dejar de recordar de nuevo que esto se consigue en base al tratamiento masivo de datos personales, y ha de advertirse que al final los datos se convierten en la contraprestación de tales servicios o información, que por tanto, y en contra de lo que los usuarios pueden llegar a pensar, no son gratuitos, sino onerosos, siendo los datos el valor de cambio por la prestación recibida. El Proyecto de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales, de 2015,[54] prevé expresamente que los datos puedan ser la contraprestación de los servicios digitales ofrecidos[55]. El artículo 3º dispone en su párrafo 1º que "la presente Directiva se aplicará a cualquier contrato en virtud del cual el proveedor suministra contenidos digitales al consumidor o se compromete a hacerlo y, a cambio, se paga un precio o el consumidor facilita activamente otra contraprestación no dineraria en forma de datos personales u otro tipo de datos". Si bien la propuesta parte de la realidad de las cosas (los datos son en no pocas ocasiones la contraprestación de servicios aparentemente gratuitos) debe advertirse acerca del riesgo que deriva del hecho de patrimonializar los datos

---

53 Vid. FERNANDEZ SAMANIEGO, Javier, y FERNANDEZ-LONGORIA, Paula, "El derecho a la portabilidad de los datos", en en PIÑAR MAÑAS (Director), *Reglamento General de Protección de Datos….., op.cit.*, págs. 257 y ss.

54 Bruselas, 9.12.2015 COM(2015) 634 final 2015/0287 (COD): http://ec.europa.eu/transparency/regdoc/rep/1/2015/ES/1-2015-634-ES-F1-1.PDF

55 El considerando 13 de la Propuesta señala:

"En la economía digital, los participantes en el mercado ven a menudo, y cada vez más, la información sobre las personas como un valor comparable al dinero. Con frecuencia los contenidos digitales no se intercambian por un precio, sino por una contraprestación diferente al dinero, es decir, permitiendo el acceso a datos personales o a otro tipo de datos. Estos modelos de negocio específicos se aplican de diferentes formas en una parte considerable del mercado. La introducción de una diferenciación dependiendo de la naturaleza de la contraprestación generaría una discriminación entre los diferentes modelos de negocio, ofrecería un incentivo injustificado a las empresas para orientarse hacia la oferta de contenidos digitales a cambio de datos. Deben garantizarse condiciones equitativas. Además, los defectos en las características de funcionamiento de los contenidos digitales suministrados por una contraprestación diferente al dinero afectan a los intereses económicos de los consumidores. Por tanto, la aplicabilidad de las normas de la presente Directiva no debe depender del precio pagado por el contenido digital específico en cuestión".

personales, alejándonos de la perspectiva, mucho más certera, del carácter personalísimo del derecho a la protección de datos, vinculado a la dignidad de la persona y por tanto, en principio, indisponible. El Supervisor Europeo de Protección de Datos ha llamado críticamente la atención acerca de la posibilidad de convertir los datos en mera moneda de cambio[56].

Además de las cuestiones relacionadas con el ***big data***, el desarrollo de las ciudades inteligentes tiene mucho que ver con la Internet de las cosas, con la llamada *Internet of things* (*IoT*).

En efecto las *Smart cities* requieren la interconexión de miles, millones de dispositivos que intercambian información entre ellos. ¿Cómo podrían ser posibles, si no, los vehículos autónomos sin conductor o la información sobre el estado del tráfico o poder conocer el tiempo que falta para que llegue a nuestra parada el autobús que esperamos? No sólo necesitamos el uso de aplicaciones en nuestros dispositivos[57], sino la interconexión de las cosas a través de sensores y controladores, que son capaces de captar e intercambiar millones de datos e informaciones. Y una vez más hemos de traer a colación la opinión del Grupo de Autoridades Europeas de Protección de Datos. En su Opinión 8/2014 sobre *Recent Developments on the Internet of Things* (WP 223), de 16 de septiembre de 2014, el WP29 llama la atención acerca de las implicaciones que para la protección de datos tiene la Internet de las cosas. Cierto que el documento sólo se refiere a tres manifestaciones de la IoT (*Wearable Computing, Quantified Self* y domótica), sin entrar

---

[56] Opinion 4/2017 sobre *The Proposal for a Directive on certain aspects concerning contracts for the supply of digital content* , 14 de marzo de 2017. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2017/17-03-14_Opinion_Digital_Content_EN.pdf

Del Supervisor Europeo son también de gran interés los siguientes documentos sobre *big data*: "Preliminary Opinion" sobre *Privacy and competitiveness in the age of big data: The interplay between data protection , competition law and consumer protection in the Digital Economy*, Marzo 2014, https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-_26_competitition_law_big_data_EN.pdf. Opinión 8/2016 sobre *Coherent enforcement of fundamental rights in the age of big data*, 23 de septiembre de 2016, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Events/16-09-_23_BigData_opinion_EN.pdf.

[57] Ver el, como todos, interesante documento del WP29 Dictamen 02/2013 sobre *Las aplicaciones de los dispositivos inteligentes*, WP 202, adoptado el 27 de febrero de 2013.

en detalle el caso de las ciudades inteligentes, pero sus conclusiones les son en gran medida aplicables. El documento asume los beneficios que para la sociedad y el desarrollo puede traer consigo la Internet de las cosas, pero advierte acerca de la necesidad de respetar la legislación de protección de datos incorporando las máximas medidas de seguridad y garantizando en todo caso el control de los datos por parte de sus titulares. Asimismo, si el tratamiento de datos se basa en el consentimiento, éste debe ser informado, libre y específico.

La propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)[58] señala expresamente en su considerando 12 que "los dispositivos y máquinas conectados se comunican cada vez más entre sí mediante redes de comunicaciones electrónicas (internet de las cosas). La transmisión de comunicaciones de máquina a máquina comporta el transporte de señales a través de una red y, por ende, constituye generalmente un servicio de comunicaciones electrónicas. Con el fin de garantizar la plena protección de los derechos a la privacidad y la confidencialidad de las comunicaciones y promover una internet de las cosas fiable y segura en el mercado único digital, es necesario aclarar que el presente Reglamento ha de aplicarse a la transmisión de comunicaciones de máquina a máquina. Por lo tanto, el principio de confidencialidad establecido en el presente Reglamento también ha de aplicarse a la transmisión de comunicaciones de máquina a máquina. También se podrían adoptar salvaguardias específicas en la normativa sectorial, como por ejemplo la Directiva 2014/53/UE". Si la propuesta sale adelante, como parece[59], quedará claro que los tratamientos de datos personales que se lleven a cabo en el marco de la Internet de las cosas quedarán expresa y claramente sujetos a la legislación europea (no olvidemos que se trata de un Reglamento, no una Directiva) sobre protección de datos en las comunicaciones

[58] Bruselas, 10.1.2017 COM(2017) 10 final 2017/0003 (COD): http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0010&from=ES

[59] Además, según el artículo 29, sería plenamente aplicable a partir del 25 de mayo de 2018.

electrónicas. Sin perjuicio, por supuesto, de que cualquier tratamiento de datos está ya sujeto al marco normativo de la protección de datos.

La Comisión Europea en su Estrategia para el Mercado Único Digital de Europa, de 6 de mayo de 2015[60], resalta que los datos masivos, los servicios en nube y la Internet de las cosas son fundamentales para la competitividad de la UE. Pero también cita los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (que reconocen, respectivamente, el derecho a la intimidad y el derecho a la protección de datos) y señala que la seguridad jurídica es importante para el despliegue de la Internet de las cosas, así como que la protección de datos aumenta la confianza en los servicios digitales. Por su parte, la Resolución del Parlamento Europeo, de 19 de enero de 2016, sobre la iniciativa «Hacia un Acta del Mercado Único Digital»[61], resalta que "la economía de los datos es clave para el crecimiento económico; subraya las oportunidades que las nuevas tecnologías de la información y la comunicación, tales como los macrodatos, la computación en nube, la internet de los objetos, la impresión en 3D y otras tecnologías, pueden ofrecer a la economía y a la sociedad, en especial si se integran en otros sectores como la energía, el transporte y la logística, los servicios financieros, la educación, la venta minorista, la fabricación, la investigación o la salud y los servicios de emergencia, y si son utilizados por las autoridades públicas para impulsar ciudades inteligentes, una mejor gestión de los recursos y la optimización de la protección medioambiental; destaca, en particular, las oportunidades que brinda la digitalización del sector de la energía, mediante contadores inteligentes, redes inteligentes y centros de datos, para una producción de energía más eficiente y flexible; hace hincapié en la importancia de las asociaciones público-privadas y se felicita por las iniciativas de la Comisión en este sentido" (Párrafo 101). Pero al mismo tiempo resalta que es principio clave el que los ciudadanos deben tener el control de sus datos (párrafo 106) y que el cumplimiento de la legislación en materia de protección de datos y las garantías efectivas de privacidad y

60 Bruselas, 6.5.2015 COM(2015) 192 final: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0192&from=ES

61 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0009+0+DOC+XML+V0//ES

seguridad tal como se definen en el Reglamento general sobre protección de datos, son fundamentales para la creación de confianza entre los ciudadanos y consumidores en la economía de los datos; aboga por el fomento de la protección de la intimidad desde el diseño y por defecto; pone de manifiesto que los datos personales requieren una protección especial y reconoce que el establecimiento de salvaguardias adicionales, como la seudonimización o la anonimización, puede mejorar la protección cuando las aplicaciones de macrodatos y los proveedores de servicios en línea utilizan datos personales (párrafo 107).

V.-A modo de conclusión.

Las ciudades inteligentes traen consigo una mejora en las condiciones de vida de las personas y pueden llegar a facilitar su sostenibilidad. En su implantación y desarrollo no sólo hemos de tener en cuenta lo que la técnica, el diseño urbano y la arquitectura puedan aportar; el diálogo con el derecho es imprescindible. Y en este escenario parecen especialmente relevantes las consideraciones en torno a la transparencia y acceso y uso de datos e informaciones públicos y en torno al respeto a la protección de datos. Transparencia pública y privacidad, dos parámetros que hace no tantos años estaban prácticamente fuera del debate jurídico, hoy son imprescindibles para el desarrollo de la sociedad y en particular para el de las ciudades inteligentes. Por eso, en el necesario diálogo que debe darse entre juristas y técnicos al definir y desarrollar las ciudades inteligentes, el acceso a la información pública en un entorno de datos abiertos y el respeto a la protección de datos han de ser especialmente relevantes. Por un lado para garantizar el acceso a los datos necesarios para ello, por otro para evitar que la protección de datos quede reducida a la nada.

La cuestión no es nada fácil de resolver porque la innovación tecnológica es imparable. Y se inserta en la vida cotidiana con extraordinaria rapidez. ¿Dónde está el límite de la innovación? ¿Qué capacidad tiene el ser humano de adaptarse a lo nuevo y de asumirlo como irreversible, de ahí a hacerlo imprescindible y por fin normal? Pongamos el caso de la geolocalización: si en un principio se consideró como un atentado a la privacidad, hoy empieza a ser para muchos algo de lo que es difícil prescindir sin detenerse a pensar en las consecuencias

que puede revestir para la protección de datos. La solución no puede ser paralizar la innovación ni obviar el derecho. Muy al contrario lo que procede es impulsar el dialogo entre derecho y técnica y tener presentes los principios esenciales de los derechos fundamentales, en particular, en lo que ahora nos interesa, de la protección de datos. A veces la solución puede venir de consideraciones no complicadas en cuanto a su aplicación. Por ejemplo, la toma en consideración de los principios de privacidad desde el diseño y por defecto. Porque en ningún caso se trata de considerar el derecho como obstáculo para el desarrollo, en nuestro caso, de las ciudades inteligentes, sino de tenerlo en cuenta para su mejor implantación.

REFLEXÕES PÓS-PANÓPTICAS SOBRE VIGILÂNCIA E CONSUMO NA SOCIEDADE DA CLASSIFICAÇÃO

Andrea Cristina Versuti[1]
Marco Aurélio Rodrigues da Cunha e Cruz[2]

> "La libertad, Sancho, es uno de los más preciosos dones que a los hombres dieron los cielos; con ella no pueden igualarse los tesoros que encierra la tierra ni el mar encubre; por la libertad, así como por la honra, se puede y debe aventurar la vida, y, por el contrario, el cautiverio es el mayor mal que puede venir a los hombres".
> *El ingenioso higalgo Don Quijote de la Mancha*, v.II, Capítulo LVIII.

INTRODUÇÃO

O ano de 2017 nos fez perder dois importantes pensadores contemporâneos. Zygmunt Bauman, nascido na Polônia (1925) mas radicado na Inglaterra, redigiu uma extensa literatura sobre sua proposta de meditar a sociedade com a premissa da "liquidez" nas relações. Stefano Rodotà, nascido (1933) e radicado na Itália, parte de uma proposta sociopolítica na vanguarda de tematizar as instituições do Direito Privado, deixando uma vasta bibliografia que repercute sobre os problemas da sociedade contemporânea.

Mesmo diante da variedade e da profundidade das análises de Bauman e de Rodotà, uma relevante problematização já tangenciou a atenção destes dois autores: a vigilância na sociedade da informação. Os

[1]Doutora em Educação com ênfase em Ciência e Tecnologia pela Universidade Estadual de Campinas (2007), Mestre em Sociologia pela Universidade Estadual de Campinas (2000) e Graduada em Ciências Sociais (Bacharelado e Licenciatura) pela Universidade Estadual de Campinas (1997). Professora na área de Educação, Tecnologias e Comunicação do Departamento de Métodos e Técnicas (MTC) da Faculdade de Educação da Universidade de Brasília (UnB). Membro do corpo permanente de docentes do Programa de Pós-Graduação em Educação da Universidade de Brasília, na linha de Pesquisa Educação, Tecnologias e Comunicação (ETEC).

[2] Doutor em Direito Constitucional pela Universidad de Sevilla (2008). Membro do corpo permanente de docentes do Programa de Pós-Graduação em Direito (Mestrado em Direitos Fundamentais) da Universidade do Oeste de Santa Catarina (PPGD UNOESC), na linha de pesquisa em Direitos Fundamentais Civis. Desenvolve suas pesquisas sobre Direitos da Personalidade, Novas Mídias e Sociedade do Consumo.

dois discursos, a seu modo, são realizados com abordagens sobre o consumo, sobre a influência das tecnologias de informação e comunicação, e com um repertório de uma "sociedade de classificação".

Este texto tem como principal objetivo examinar, por meio de uma metodologia analítica, as conexões entre a obra "A vida na Sociedade da Vigilância" de Rodotà e "Vigilância Líquida" de Zygmunt Bauman, traçando um diálogo com a discussão de outros autores sobre a sociedade de consumo e suas especificidades. O trabalho está categorizado em tópicos que discutem o que cada autor estima como pressuposto para configurar o conceito de vigilância. Em seguida, coteja-se tais conceitos no marco da hipótese pós-panóptica defendida por Bauman. Ao final, como contributo principal desta reflexão, apresenta-se o argumento de que na modernidade, a vigência do panóptico estava pautada pela imobilidade e pelo aprisionamento, enquanto que na modernidade líquida, a hipótese do pós-panóptico é sustentada com a mobilidade, com o monitoramento à distância e com a servidão voluntária.

1. A VIGILÂNCIA LÍQUIDA DE ZYGMUNT BAUMAN

O diálogo entre David Lyon e Zygmunt Bauman travado no livro *Vigilância Líquida* (2014b) pretende investigar as origens históricas e ocidentais da vigilância atual e sugerir questões éticas, assim como políticas, sobre sua expansão. Reporta-se aos debates sobre o projeto pan-óptico da vigilância e dos inventos contemporâneos da globalização, os quais não deixam lugar para a ocultação. A linha argumentativa declina premissas para auxiliar a compreensão do que ocorre com o monitoramento, com o controle, com a observação, com a classificação, com a checagem e com a atenção sistemática do que se pode chamar de vigilância. (BAUMAN, 2014b).

Acolhe-se que a vigilância é uma dimensão central da modernidade. Esta modernidade "tardia", "pós-modernidade", ou como Bauman propõe: "modernidade líquida". (BAUMAN, 2014b, 2001). Esta proposta de "liquidez" e "fluidez" arvora-se na afamada construção frasal de "derreter os sólidos", forjada pelos autores do "Manifesto Comunista" e reiterada por Marshall Berman em "*Tudo que é sólido desmancha no*

ar: a aventura da modernidade" (1982), para metaforizar a presente fase na história da modernidade; na qual ideias sólidas seriam diluídas da mesma forma que os materiais sólidos (BAUMAN, 2001). Os líquidos alteram sua forma, não fixam o espaço e tampouco prendem o tempo. Os sólidos possuem dimensões espaciais claras e, por isso, resistem ao tempo. Os fluidos são caracterizados, também, por sua mobilidade e inconstância, pois fluem, esvaem-se, contornam, invadem, inundam. (BAUMAN, 2001).

A mobilidade como característica contemporânea já foi abordada, sob outra ótica, por outros autores. Principalmente com o foco na informação. Santaella (2007), por sua vez, analisa que a era da comunicação móvel é marcada pelo desaparecimento progressivo dos suportes, o que faz com que a comunicação, os fluxos dos signos e as trocas de informação se desprendam dos lugares fixos. Estes novos modelos de telecomunicações interferem diretamente na nossa percepção cotidiana, seja do tempo, do espaço, dos modos de viver e aprender, porque o mundo *online* propicia recursos que ajudam a sustentar a programação mais complexa que em outros meios de comunicação. (JOHNSON, 2001).

Bauman (2011) assevera que o mundo líquido moderno é um mundo de surpresas, pois o correto e adequado de hoje, amanhã pode se converter em fútil, fantasioso e dotado de equivocidade. Esta alteração se reflete na sociedade. Com a suspeita de alteração, os indivíduos partem da ideia de que devem estar sempre prontos a mudar, ser flexíveis. E esta flexibilidade conduz a uma busca por informações sobre o que ocorre e o que poderá ocorrer. Segundo Bauman (2011, p. 8), a Internet como "autoestrada de informação" nos conecta instantaneamente e "em tempo real" a todo e qualquer canto remoto por meio dos dispositivos móveis que carregamos, dia e noite, para onde nos deslocamos. A ausência da informação insuficiente da "sociedade dos produtores" foi substituída pela abundância de informações, "que ameaça nos afogar, nos impede de nadar ou mergulhar" (BAUMAN, 2011, p. 8).

Lev Manovich (2001, p.114), define que a interface molda a própria concepção do ser humano e "determina también el modo en que piensa em cualquier objeto mediático". O autor afirma que a interface impõe sua própria lógica de organizar os dados. A interface transporta

informações culturais, e quando se está na Internet essas informações passam por interfaces interativas, mas estas informações dificilmente chegam até ao receptor de forma neutra.

Do ponto de vista técnico e operacional, alguns fatores explicam a convergência associada aos aparatos e dispositivos, pois, com os avanços tecnológicos da última década, há meios de se estar conectado todo o tempo, e em qualquer lugar, desde que esteja com o celular em mãos. Além da possibilidade de se estar conectado a rede em tempo integral, a informação chega até os indivíduos através de diversas formas como, texto, imagem, vídeos e som. Neste sentido, qualquer equipamento que consiga conectar-se à rede torna-se então um veículo de comunicação capaz de converter vários formatos de informação em um só equipamento.

A partir disso, podem ser imediatamente observadas as várias facetas de informação que um só receptor vai adquirindo na medida em que passa de uma mídia para a outra: de ouvinte a espectador, de espectador a leitor, enquanto gradualmente forma sua opinião acerca da realidade a partir da multiplicidade de fontes. (SANTAELLA, 1996, p.38).

Com celulares computadorizados multifuncionais cada vez mais velozes, tornando-se "pequenas criaturas sensíveis, quase vivas" (SANTAELLA, 2007, p.232) ou talismãs simbólicos (GERGEN, 2003, p.107) colados ao corpo, respondentes ao toque como uma prótese portátil, personalizada e amigável permitindo acessar qualquer pessoa em qualquer parte do mundo ou experienciar a presença-ausência, a cooperação com vizinhanças virtuais e a troca de arquivos, visualiza-se a emergência simultânea de dois conceitos importantes: mobilidade e convergência. Com estes equipamentos é possível ter a vivência da ubiquidade e do nomadismo por meio de uma tecnologia colaborativa personalizada, pois para Santaella (2007, p. 234) "não é o equipamento que necessariamente define a mobilidade, mas o tipo de comunicação", comunicação esta caracterizada pela disponibilização, exposição, troca e colaboração. (AUGÉ, 1990).

Dentro deste contexto de mobilidade, flexibilidade e fluidez, Bauman (2001) advoga que há uma redistribuição e realocação dos "poderes de derretimento" da modernidade, que interfere nas instituições, nos moldes que delimitavam o domínio das "ações-escolha" possíveis, nas configurações, nos padrões de dependência e de interação.

Há um "fluido" refazimento e uma "líquida" substituição por nova moldura de tais caracterizações da sociedade. Isso refletiu nos padrões, códigos e regras que nos conformavam, antes pontos estáveis de orientação e guia, hoje deveras escassos. Estes "poderes em derretimento" ou em liquefação trasladaram do "sistema" para a sociedade, da política para o convívio social. (BAUMAN, 2001). Neste mundo "líquido moderno", Bauman (2001) contrasta cinco conceitos básicos das narrativas da condição humana com as atuais transformações: a emancipação, a individualidade, o tempo/espaço, o trabalho e a comunidade. Neste sentido, Bauman (2011, p. 7) sustenta, portanto, a liquidez ou a fluidez pois "[...] O mundo que chamo de <líquido> porque, como todos os líquidos, ele jamais se imobiliza nem conserva sua forma por muito tempo. Tudo ou quase tudo em nosso mundo está sempre em mudança [...]".

Em *Vigilância líquida,* Bauman (2014b) ressalta duas características com as quais lida a modernidade líquida. A primeira se refere ao "derretimento" mais rápido das formas sociais do que a velocidade com que novas formas são criadas. Disso decorre que seus moldes não se constituem referência para as ações e as estratégias dos seres humanos, dada a brevidade de sua "vida útil". A afetação desta premissa na vigilância direciona para uma postura mais móvel e flexível, infiltrando-se e se espalhando em muitas áreas da vida.

A "arquitetura" da vigilância capta os dados convertendo-os em "duplicatas de dados", potencialmente móveis e fluidos, encontradiços em culturas permeadas pela fragmentação e pela incerteza. Bauman (2014b) sublinha que o projeto pan-óptico matinha o controle ao imobilizar os prisioneiros e promover movimento dos observadores. Por isso sua proposta é de que o mundo líquido é pós-panóptico, pois neste a mobilidade e o nomadismo são valorizados. O poder se afirma mediante as tecnologias eletrônicas que conformam as mutáveis e móveis organizações atuais, o que problematiza a arquitetura de paredes e janelas, de fronteiras. As diversas e diferentes formas de controle não têm uma conexão direta com o aprisionamento e, ademais, comungam das características de flexibilidade e de diversão estimuladas pelo entretenimento e pelo consumo.

Outra importante característica da modernidade líquida, segundo Bauman (2008a), é a separação entre poder e política. Há

presença do poder num espaço desterritorializado, mas a política continua local, incapaz de agir em nível global. A transmissão instantânea de informação leva a não se ignorar a mídia eletrônica, sob pena de se basear na mídia ortodoxa, recheada de reuniões e conversações de velocidade com "limites naturais", com custos altos e comparativamente crescentes. (BAUMAN, 2008a). O resultado é a desvalorização do lugar e a desterritorialização do poder. "O espaço físico, não cibernético, onde as comunicações não-virtuais ocorrem, é apenas uma lugar para entrega, absorção e reciclagem da informação do ciberespaço, essencialmente extraterritorial". (BAUMAN, 2008a, p. 44). O poder sem controle político, portanto, converte-se em fonte de incerteza, enquanto a política augura pouca importância para os problemas da vida das pessoas. O poder de vigilância também se aloca nesta descrição. A combinação das formas sociais e da separação entre poder e política caracterizam a modernidade líquida e, portanto, repercutem na vigilância.

De acordo com Aguero (2008):

> A Sociedade de Controle estaria identificada com mudanças que aconteceram por todo o mundo capitalista, ligadas principalmente às inovações tecnológicas. O uso dessas novas tecnologias para o controle social seria a mais nova expressão do exercício do poder na sociedade moderna. Os mecanismos de vigilância aprimoraram-se e passaram de um caráter institucional para o de uma vigilância geral. A proliferação de câmeras de vídeo em muitos espaços sociais, o uso de *transponders*, de aparelhos celulares, cartões de crédito e da comunicação pela Internet facilitaram o exercício de mecanismos de vigilância e controle cada vez mais eficientes. Embora esse paradigma de sociedade possa ser compreendido como uma derivação da sociedade disciplinar foucaultiana, dela se diferencia quando o controle passa de uma esfera local, dos espaços fechados das instituições, para todos os campos da vida social. [...] (AGUERO, 2008, p.35-36).

No modelo social questionado por Deleuze (2010), o controle sai do âmbito local – restrito à extensão dos olhos e do ouvido humanos-, para um âmbito supra-local, estendendo-se a todos os espaços da vida pública. Sendo assim, é mais perverso, mais controlador, porque se sustenta no aparato das novas tecnologias de informação, que operam por continuidade e comunicação instantânea. A simbologia do controle

agora "[...], [é] a rede digital de comunicação mundial, que concentra toda a informação dos indivíduos em bancos de dados. O princípio da docilidade continua, [...] pois os indivíduos entregam voluntariamente seus dados à vigilância". (AGUERO, 2008, p. 35-36).

Deleuze (2010) aponta que na "Sociedade de Controle" só os muros declinaram, porque a ideologia de confinamento não colapsou com estes. Dentro desta mesma lógica, também perde força a noção de indústria/fábrica e ascende a noção de empresa, aparentemente muito mais flexível e polimorfa. O ser humano confinado da "Sociedade Disciplinar", na "Sociedade de Controle", ganha *status* de ser endividado. Isto porque o estímulo ao consumismo exacerbado produz cada vez mais pessoas com imensas dívidas monetárias. Assim como o confinamento, o endividamento é um mecanismo eficaz de sujeição estimulado pela produção de subjetividade capitalística (GUATTARI, 1992). Assim, o controle pelo consumo caracteriza-se como a nova forma mais sutil de dominação. Porque o que se consome não são somente coisas, mas, as formas de ser, pensar, agir, produzir e se relacionar.

Bauman (2001, 2014b) pugna que na modernidade líquida, o poder flui, flutua sobre os territórios e as fronteiras, com os postos de controle sendo superados ou contornados. As redes de vínculos sociais, especialmente com base no território, são afetadas por esta "liquidez". E Bauman (2008b, 2014b) dá o exemplo da conexão mútua entre as novas mídias e os relacionamentos fluidos. Para a sua construção, a mídia social é dependente de um sistema que monitore os usuários e venda de seus dados para outros. Por "cortesia" da internet, há consentimento em "vender" o direito à privacidade, como preço pelos benefícios ofertados em troca. Bauman (2014b, p.22) acredita que a pressão social por essa mitigação da autonomia pessoal é tão intensa "tão próxima à condição de um rebanho de ovelhas, que só uns poucos excepcionalmente rebeldes, corajosos, combativos e resolutos estejam preparados para a tentativa séria de resistir". Com esta "renúncia" consentida à privacidade Bauman (2014b) aproxima uma "erosão do anonimato", pois tudo que antes era privado, nas mídias sociais tem efeito potencialmente público, e está disponível para o consumo público. A "erosão do anonimato", portanto, provém dos serviços da mídia social e de uma mudança de entendimento dos usuários do que deve ser público e do que deve ser privado.

Antes "privado" e "público" possuíam um antagonismo nos raios semânticos, dissociados por limites demarcados para evitar invasões ou transgressões. (BAUMAN, 2011). Esta demarcação priorizava o direito ao controle e a decisão sobre quem e o que teria a permissão de passar deste limite, e o que deveria permanecer de um dos lados. A esta modificação do que haveria de ser considerado público e privado pelos "usuários" Bauman (2014b) conecta as inquietações sobre a servidão voluntária de Étienne de la Boétie (2017) e das projeções pan-ópticas de Michel Foucault (2010), que serão trabalhadas no último tópico deste texto. Entretanto, antes de comentar sobre esta conexão, urge explanar as premissas sobre as quais Bauman (2014b) a sustenta.

A primeira é a afirmação de que a vigilância contemporânea logrou; com o monitoramento, o controle, a observação, a classificação, a checagem dos usuários e "venda" de dados pessoais; estabelecer uma servidão do tipo <faça você mesmo>, em que se consente, por vontade própria, trabalhar a serviço de uma mesma realidade. O estratagema pan-óptico (você nunca vai saber quando é observado, nunca imagine que não está sendo espionado) é implantado, aos poucos, em escala global. Contudo, altera-se o <Nunca estou sozinho> para o esperançoso <Nunca mais vou ficar sozinho> (abandonado, ignorado, desprezado, excluído), o medo da exposição é intercambiado pela alegria de ser notado. A visibilidade, antes uma ameaça, foi reclassificada para uma tentação, ou um desejo. A exposição se converte na prova de reconhecimento social, ao ponto de Bauman fazer uma releitura do *cogito* de Descartes: "sou visto (observado, notado, registrado), logo existo". (BAUMAN, 2014b, p. 105). Sobre a tomada de poder da subjetividade, Félix Guattari e Suely Rolnik (1996) já afirmaram que:

> A cultura como esfera autônoma só existe a nível dos mercados de poder, dos mercados econômicos, e não a nível da produção, da criação e do consumo real. O que caracteriza os modos de produção *capitalísticos* é que eles não funcionam unicamente no registro dos valores de troca, valores que são da ordem do capital, das semióticas monetárias ou dos modos de financiamento. Eles funcionam também através de um modo de controle da subjetivação, que eu chamaria de "cultura da equivalência" ou de "sistemas de equivalência na esfera da cultura". Desse ponto de vista o capital funciona de modo complementar à cultura enquanto conceito de equivalência: o capital ocupa-se da sujeição econômica, e a cultura, da sujeição subjetiva. E

> quando falo em sujeição subjetiva não me refiro apenas à publicidade para produção e consumo de bens. É a própria essência do lucro capitalista que não se reduz ao campo de mais-valia econômica: ela está também na tomada de poder da subjetividade. (GUATTARI e ROLNIK, 1996, p. 15-16).

Neste sentido, a "máquina" capitalística produz tudo, inclusive os sonhos, devaneios, fantasias, paixões e assim por diante. (GUATTARI e ROLNIK, 1996). Assim, a subjetividade não é passível de totalização ou de centralização no indivíduo, mas se estabelece como produção incessante, através dos agenciamentos das forças que atravessam as relações, como o outro social, a natureza, os acontecimentos, as invenções, tudo aquilo que produz efeitos nos corpos e nos modos de viver. Guattari aponta que a "subjetividade é essencialmente fabricada e modelada no registro do social" (GUATTARI; ROLNIK, 1996, p. 31).

Sobre o "refazimento" da subjetividade, Bauman (2014b) traça um paralelo do reconhecimento social com as confissões. David Lyon dialoga com as ideias de Foucault sobre a confissão, a qual havia se tornado um critério para a verdade, pois extraída do âmago do ser de uma pessoa. Esta assertiva, portanto, entendia que os indivíduos têm um participação ativa na sua própria vigilância. Não se avança na análise sobre se Foucault consideraria ou não os *perfis* ou *blogs* uma confissão, mas Bauman (2014b) diferencia a compreensão pré-moderna da confissão, como admissão de culpa; da moderna, como manifestação, exteriorização e afirmação de uma "verdade interior", um sustentáculo da individualidade e da privacidade do indivíduo. Se antes o segredo e o sigilo delimitavam a fronteira da privacidade, o domínio da própria pessoa; hoje as mídias sociais forçam uma condição caracterizada de ouvintes ávidos por remover os segredos e sigilos que se ocultam por detrás desta fronteira, levando a privacidade a um local de encarceramento. (BAUMAN, 2014b, 2011). Neste contexto de confissões, Bauman (2014b) observa a atual "sociedade confessional", em que se elimina a fronteira de separação entre o privado e o público ao se fazer a exposição pública do privado, mediada pela lógica da "Sociedade de Consumidores".

Featherstone (1995) já chamou a atenção para importantes mudanças[3] ocorridas na cultura no contexto contemporâneo. Tais transformações incluem as práticas e experiências cotidianas de diferentes grupos e sua utilização dos regimes de significação, bem como o desenvolvimento de novos meios de orientação e estruturação das identidades. O autor considera relevante uma reflexão acerca da proeminência cada vez maior da "cultura de consumo", ou seja, o reconhecimento de um estreito relacionamento entre cultura, economia e sociedade, não considerando o consumo como derivado direto e negativo da lógica da produção. É preciso analisar as questões de desejo, prazer, satisfações emocionais e estéticas derivadas da experiência do consumo e não restringi-las apenas em termos de manipulação ideológica.

Além disso, é preciso considerar ainda o aspecto duplamente simbólico das mercadorias; seu simbolismo não está apenas no imaginário embutido nos processos de produção e marketing, mas também nas renegociações utilizadas para enfatizar diferenças de estilos de vida, demarcado as relações sociais. A partir do consumo, pois, articula-se um universo de significações que por sua vez significam e (re)significam as práticas cotidianas, pois os elementos utilizados neste processo são dotados de legitimidade no sentido em que mobilizam símbolos de um imaginário internacional-popular alimentado pela publicidade.

No consumo ocorre a construção de identidades a partir de símbolos com significados específicos e que são comunicados com outros grupos. A beleza das imagens publicitárias, as mudanças no seu tratamento, sua multiplicidade, simultaneidade e riquezas de informação trazidas a um tempo ínfimo, a utilização de sensações, o apelo ao deslumbramento visual de paisagens, modelos, carros, entre outros, estão associados a estes fenômenos sociais decorrentes do processo de informatização da sociedade com exigências de um consumo exacerbado, o consumismo.

---

[3] É importante ressaltar que estas transformações não devem ser pensadas como rupturas ao modelo de organização econômica capitalista moderno, mas sim como suas consequências diretas causadas pela radicalização de alguns de seus princípios fundamentais. *Cfr*: GIDDENS, Anthony. **As consequências da modernidade.** SP: Unesp,1991.

Este consumo supõe a manipulação ativa de signos (BAUDRILLARD, 2008) que muitas vezes independem dos objetos concretos e podem estar disponíveis em uma multiplicidade de relações associativas, bastante exploradas pela mídia e de forma mais especial e enfática pela publicidade. Consumir remete diretamente à ideia de pertencimento social, seja este concreto ou apenas visual, seja pelo consumo direto ou pelo consumo de imagens, isto não importa, o relevante é estar inserido em uma certa imposição de contemporaneidade e de certa forma estar conectado às transformações de seu tempo. "Assim, as mercadorias ficam livres para adquirir uma ampla variedade de associações e ilusões culturais". (FEATHERSTONE, 1995, p.33).

Efetivamente, a lógica da "Sociedade de Consumidores" é retratada por Bauman (2008b) em "*Vida para o consumo: a transformação das pessoas em mercadoria*". A principal razão que estimula o engajamento de uma incansável atividade de consumo é sair da invisibilidade e da imaterialidade para se destacar e se diferenciar da "massa de objetos indistinguíveis <que flutuam com igual gravidade específica" e assim captar o olhar dos demais consumidores. (BAUMAN, 2008b, p.20-21). Se antes na "Sociedade de produtores" havia o pressuposto do "fetichismo da mercadoria", o hábito de, por ação ou omissão, ignorar ou esconder a interação humana por trás do movimento das mercadorias; na "Sociedade de consumidores" vige o fetichismo da subjetividade, em que se compra e vende "os símbolos empregados na construção da identidade - a expressão supostamente pública do <self> que na verdade é o <simulacro> de Jean Baudrillard, colocando a <representação> no lugar daquilo que ela deveria representar". (BAUMAN, 2008b, p.23-24).

Baudrillard (1981), analisa as sociedades ocidentais contemporâneas a partir do consumo de objetos. Afirma que o consumo surge como modo ativo de relação (não só com objetos, mas ainda com a coletividade e com o mundo), "como modo de atividade sistemática e de resposta global, que serve de base a todo o nosso sistema cultural". (1981, p. 11). Tanto na lógica dos signos como na lógica dos símbolos, Baudrillard (1981) parte do pressuposto de que os objetos não se prestam mais a conectar à funções ou necessidades definidas, pois respondem a uma lógica social ou a uma lógica do desejo, às quais

servem de campo móvel e inconsciente de significação. O consumo, nesta linha de raciocínio, se desloca para ser inserido na moral contemporânea.

Bauman (2014b) retoma esta lógica em *Vigilância líquida*, pois adverte que a vigilância contemporânea, com monitoramento, o controle, a observação, a classificação, a checagem e a "venda" (consumo) de dados, conseguiu que os indivíduos, com a servidão do <faça você mesmo>, sejam simultaneamente promotores de produtos e os produtos que promovem. Os "usuários" são, ao mesmo tempo, as mercadorias e os agentes de marketing, os produtos e os vendedores itinerantes, para que augurem uma visibilidade e, porventura, <valor social> e/ou autoestima.

Para Bauman (2014b, p. 100) uma das características do avanço da sociedade consumista foi a passagem da produção direcionada para a demanda existente, de satisfação de necessidades; para a demanda voltada para a produção existente (a sua criação) "por meio de tentação, sedução e estímulo do desejo assim despertado". Busca-se, portanto, o direcionamento de ofertas a pessoas ou categorias de pessoas já previamente prontas para aceitá-las, entusiasmadas. A dispendiosa estratégia de marketing de despertar desejos foi transferida para os potenciais consumidores. E é nesta nova perspectiva que Bauman (2014b) insere a tecnologia de vigilância, do controle, da observação, da classificação, da checagem e da atenção sistemática aos dados dos usuários, para comercializá-los na lógica do consumo. Os assuntos relativos à segurança e à vigilância com a lógica do consumo, tendem a ser tratados com mais liberdade, pois:

> Afinal, esse é o domínio da diversão, do *flâneur*, da liberdade. [...] Aqui encontramos uma detalhada operação gerencial, baseada uma vez mais na coleta de dados pessoais em grande escala, com o objetivo de concatenar, classificar e tratar de formas diversas diferentes categorias de consumidores a partir de seus perfis. (BAUMAN, 2014b, p. 98).

O paradoxo, levantado por David Lyon no diálogo com Bauman, é que "embora o consumo exija a prazerosa sedução dos consumidores, essa sedução é também resultado de vigilância sistemática numa enorme escala". (BAUMAN, 2014b, p. 98).

Estas assertivas sobre a arquitetura da vigilância podem ser conectadas com os meios informativos pelos quais o consumo tem sido "entusiasmadamente" estimulado. De acordo com Almeida (2001), assiste-se à formação de uma nova oralidade na qual os meios de comunicação formam a lógica do entendimento do mundo destes novos indivíduos. Esta nova oralidade impõem o reconhecimento das diferentes relações que agora são estabelecidas entre os sujeitos com e através da linguagem audiovisual. "O visual torna-se assim o centro polimórfico que deve ser interpretado e o meio da interpretação. O visual é o objeto e o método." (CANEVACCI, 1995, p.44). Deve-se considerar também como esta oralidade introduz novos instrumentos para pensar a vida cotidiana, abrindo novas formas de entendimento acerca da realidade social ao lidar de modo convincente e peculiar com novas categorias de tempo e espaço. A realidade peculiar das imagens apresenta uma nova construção significativa do conhecimento, entendido como algo contínuo, mas ao mesmo tempo presentificado através de uma particular elaboração do tempo.

O mundo que se apresenta cada vez mais é o do consumo ampliado de imagens trazido pelo alargamento do campo sensitivo, maximizando a visibilidade. Este novo olhar lançado sobre o universo das imagens fascina-se pela difusão da ideia de instantaneidade e simultaneidade na qual as imagens aparecem múltiplas, híbridas. A estética da saturação exige uma máxima concentração de informações em um mínimo espaço de tempo, o que impossibilita uma leitura linear das imagens. (MACHADO, 1993). O processo de comunicação, bem como a transmissão de qualquer tipo de conteúdo, deve ser concebido como uma articulação de práticas de significação, num campo de forças sociais pertencentes a um certo conjunto de sentidos disponíveis na sociedade.

As mídias, através de um estilo rápido que cria a aparência de variabilidade e inovação (SARLO, 1997) prendendo de modo infatigável a atenção de seus interlocutores, passam a ser um dos componentes essenciais na definição dos comportamentos, sentimentos, sentidos e ações, ditando como principal regra o consumo, impondo e fabricando um novo tipo de imaginário social no qual a maioria restringe-se ao mero consumo de imagens, enquanto uma minoria pode ter acesso aos bens concretos.

De acordo com Jameson (1996) e Featherstone (1995) é possível reconhecer outras categorias para pensar a linguagem e os sistemas simbólicos de (re)significação do mundo contemporâneo: os indivíduos são levados cada vez mais a penetrar a materialidade das palavras em direção ao seu sentido em uma busca que se torna obsessiva e constante, pois muitos dos significantes concretos que perderam seu significado foram transformados em imagens, que passam a ser os novos referenciais, apresentando um relacionamento intrínseco entre produção cultural e a generalidade da vida social. Nesse contexto, marcado pela instantaneidade, mobilidade e fluidez das imagens, surgem novos produtos e bens simbólicos e com eles, novos tipos de consumo, de instrumentos "sociais" de pertencimento, de obsolescência programada, de "regulamentos" de relações intersubjetivas, e, inevitavelmente de novos sistemas de vigilância e de controle para manutenção desta lógica da visibilidade, como a vigilância líquida.

2 A SOCIEDADE DA VIGILÂNCIA (E DA CLASSIFICAÇÃO) DE STEFANO RODOTÀ

Em "*Vigilância Líquida",* Bauman (2014b) ainda assinala duas questões sobre a ética da segurança, com a quais trabalha o conceito de "adiaforização". A primeira é a tendência a "adiaforização" em que sistemas e processos se divorciam de qualquer consideração de caráter moral. O conceito de "adiaforização" é mais detalhado em "*Cegueira Moral: a perda da sensibilidade na Modernidade Líquida*" (2014a) em que se discute com Leonidas Donskis a perda da sensibilidade moral e uma possibilidade de releitura (redescoberta) do pertencimento como alternativa viável à fragmentação, à atomização e à "individualização" da sociedade. Bauman (2014a) utiliza o conceito de insensibilidade moral para incluir a conduta indolente, indiferente, implacável e desumana, assumida e expressada nas respostas aos problemas de outras pessoas. Aponta-se, portanto, uma incapacidade de notar estímulos em condições "normais", uma insensibilidade (des)encontrada nas relações entre os seres humanos, e portanto morais. O processo de individualização conduz a ocorrências em que são prescindíveis avaliações e regulações

morais. E desta exclusão (isenção) do domínio da avaliação moral, Bauman (2014a) forja o conceito de "adiaforização".

A variável da "liquidez" na adiaforização se insere no padrão relacional "consumidor-mercadoria", reproduzido nas relações intersubjetivas. Não se projeta uma lealdade perene à mercadoria, apenas uma satisfação das necessidades ou desejos. Busca-se a utilização dos produtos e serviços do mercado de consumo enquanto atendam às expectativas, não mais que isso. Se encontrados outros produtos e serviços que melhor satisfaçam os mesmos desejos, estes bens de consumo são "duráveis", intercambiáveis, e, portanto, dispensáveis perante a lógica do consumo. Logo, a longevidade da utilização dos bens de consumo tende a ser aligeirada, inversamente proporcional à frequência da rejeição e do descarte. (BAUMAN, 2014a).

Em *Vigilância Líquida* (BAUMAN, 2014b), David Lyon, no debate com Bauman, comenta que Gary Marx se propôs a descrever estratégias de intervenção jurídica e regulatória para a difusão da vigilância. Foi Gary Marx, segundo Lyon, que insistiu na expressão "suspeito categórico", em que se classifica com softwares e estatísticas quem é de interesse para a polícia.

> Cada vez mais os corpos são <informatizados>. [...] a informação sobre esse corpo está sendo tratada como se fosse conclusiva na determinação da identidade da pessoa. [...] isso dá outra volta orientada para a vigilância naquilo que você fala sobre adiaforização, as ações isentadas de avaliação ética por meios técnicos. A mediação eletrônica permite um distanciamento maior entre ator e resultado do que se poderia imaginar na burocracia pré-digital [...]. (BAUMAN, 2014b, p. 107-109).

Deste diálogo, Bauman (2014b) leva a perspectiva classificatória da vigilância líquida, que emprega a "manipulação pela escolha (pela sedução, não pela coerção)" como método mais seguro para modular as ofertas por meio da demanda. A colaboração voluntária (servidão do <faça você mesmo>) e exaltada é o primordial recurso utilizado pelos mercados de consumo:

> "[...] Reempregada em nome da inclusão da <livre escolha> na estratégia de marketing, ou, mais precisamente, de tornar voluntária a servidão e fazer com que a submissão seja vivenciada como um avanço

> da liberdade e um testemunho da autonomia de quem escolhe". (BAUMAN, 2014b, p.110).

Se o ser humano é classificado ou tratado com uma mercadoria selecionada, segundo cor, tamanho e números, Bauman (2014b) reputa que a adiaforização é mais devastadora. Isso porque se decompostas, fatiadas, pulverizadas e/ou atomizadas as características para posteriormente "recompô-las" para a construção de um estereótipo conveniente "[...] Qualquer que seja a função manifesta desse exercício, sua função latente, mas indetectável, é a exclusão do objeto da decomposição/recomposição da classe de entidades moralmente relevantes e do universo das obrigações morais". (BAUMAN, 2014b, p. 111).

A segunda preocupação sobre a ética da segurança e a sua "adiaforização" gravita sobre o distanciamento. Isso porque vigilância torna mais eficiente o processo de fazer coisas a distância, de separar uma pessoa das consequências de sua ação. Este ângulo da adiaforização, em termos de vigilância, é explorado como os dados do corpo (dados biométricos, DNA, etc) ou por ele desencadeados são coletados para bases de dados a fim de serem organizados, examinados, e sistematizados com outros dados e depois devolvidos como "replicação de dados". As informações da pessoa são constituídas de "dados" apenas no sentido em que se originaram em seu corpo e podem afetar suas oportunidades e escolhas existenciais. A atomização e replicação dos dados inspira maior confiança do que a própria pessoa ao contar sua própria história. Os "cientistas de dados" os "designers de software" podem se refugiar no argumento de que estão simplesmente <lidando com dados>, de modo que seu papel é "moralmente neutro", e suas avaliações, classificações e distinções são apenas "racionais". A vigilância líquida, portanto, "pode anular alguns escrúpulos morais ao manifestar suas <aplicações de proteção>". (BAUMAN, 2014b, p. 114).

Esta perspectiva classificatória, sob outra ótica, já foi suscitada por Jean Baudrillard (1981) na caracterização da lógica social do consumo. Baudrillard (1981) afirma que a lógica social do consumo não é a da apropriação individual do valor de uso dos bens e dos serviços; tampouco é a lógica da satisfação; mas é a lógica da produção e manipulação dos significantes sociais: a lógica da diferenciação. O

processo de consumo pode ser analisado nesta perspectiva sob dois aspectos fundamentais: (1) como processo de significação e de comunicação, baseado num código em que as práticas de consumo se inserem e assumem um respectivo sentido de sistema de permuta e de equivalência a uma linguagem; (2) como processo de classificação e diferenciação social, em que os objetos/signos se ordenam, não só como diferenças significativas no interior de um código, mas como valores estatutários no seio de uma hierarquia. Aqui reside, portanto uma lógica da diferenciação, que leva a referir-se a outros signos. A lógica da diferenciação, portanto, produz os indivíduos como "personalizados", como diferentes dos demais, mas consoante os modelos gerais e respeitando um código aos quais se amoldam. As diferenças codificadas, longe de dividir os indivíduos, tornam-se antes material de troca e de classificação/diferenciação.

Nesta perspectiva também destacam-se os trabalhos de Pierre Bourdieu (2007) sobre a "distinção" social, acerca das diferentes estratégias de pertencimento e diferenciação desenvolvidas pelos grupos sociais e que envolvem o campo não somente econômico, mas sobretudo o campo simbólico e o campo cultural. Para o autor, um estilo de vida se configura na o apenas como uma maneira de se comportar, mas tambe m, e principalmente como um julgamento sobre o mundo, como uma forma de se diferenciar nele. A distinção representa em suma os esforços em manter a exclusividade de uma posiça o social dominadora, atrave s do contraste com os si mbolos da mediocridade de uma condiça o de subordinaça o. De uma parte, o "distinto", porque quantitativamente raro, ou porque na o compromissado com necessidades materiais, e que, justamente por isso, pode ser o marco dos bens e das condutas de vida das fraço es sociais dominantes, as quais na o esta o submetidas a essas necessidades. De outra, o "vulgar", porque de fa cil aquisiça o ou porque ligado a exigências prima rias, cuja satisfaça o e o principal desafio para os dominados. No meio, as pra ticas destinadas ao julgamento, por via da distância entre as ambiço es e as possibilidades. Pelos gostos, desenvolve-se uma batalha simbo lica para a apropriaça o das posiço es de domi nio, de pertencimento, de adimplemento de "regulamentos" de relações intersubjetivas, e, portanto, de diferenciação e classificação.

Uma "Sociedade da Classificação" também já foi vislumbrada por Stefano Rodotà em *"A vida na sociedade da vigilância"* (2008, p. 111-140). Uma das primeiras indagações sobre sua meditação da configuração da "Sociedade da Classificação" é: "Sociedade da vigilância total ou sociedade da liberação total? Devemos nos concentrar na multiplicação de sistemas e ocasiões de controle ou na liberdade anárquica que se encontra (ou que se espera encontrar) nas redes?". (RODOTÀ, 2008, p. 111).

Para responder ao questionamento sobre a "Sociedade da Classificação", Rodotà (2008) prioriza o contexto em que se constituem as relações intersubjetivas, entre pessoas e organizações, e entre as organizações. Admite que na maioria das relações mediadas na e pela Internet são produzidos os *transactional data* ou *telecomunications-related personal informations* (TRPI). Tais dados são constituídos pela relação contratual e permitem a aquisição automática de uma série de informações do consumidor ao fornecedor de serviços ou produtos. Tais dados (identificação, local, horário, forma de pagamento, modo de utilização de serviço) se configuram também informações sobre as escolhas e preferências.

As informações, pois, podem ser consultadas quando ao fornecedor/prestador lhe aprouver, para finalidades estatísticas, para planejamento de campanhas publicitárias ou para cessão a terceiros. Portanto, além da soma de dinheiro, há uma contraprestação inerente ao se obter um produto ou um serviço na maioria das relações mediadas na e pela Internet: a cessão das informações pessoais. As relações comerciais não são mais pautadas apenas pela simples operação econômica. Para o serviço ser prestado ou para o produto ser adquirido a pessoa é obrigada a expor a sua *persona* representada pela *posse* do fornecedor/prestador/detentor das suas informações pessoais.

Ademais, os "perfis dos usuários" vão sendo alimentados pelo seu histórico de consumo. Estes "rastros" deixados pelo consumidor fazem parte da perspectiva gerencial do sistema de vigilância sobre os usuários. (RODOTÀ, 2008). A vigilância, pois, permeia o cotidiano e se torna uma característica das relações de mercado "cuja fluidez diz respeito à possibilidade de dispor livremente de um conjunto crescente de informações". (RODOTÁ, 2008, p. 113).

De fato, pode-se cotejar esta perspectiva de vigilância de Rodotà (2008) com a vigilância líquida de Bauman (2014b). A convergência das duas propostas se desvela no discurso de que o monitoramento, o controle, a observação, a classificação, a checagem e a atenção sistemática aos dados e informações dos "usuários" fazem parte do aparato de vigilância e são estruturantes do sistema. Em uma paráfrase com a sociedade de controle de Deleuze (2010), "Não se está mais diante do par massa-indivíduo. Os indivíduos tornaram-se '*dividuais*', divisíveis, e as massas tornaram-se amostras, dados, mercados ou *bancos*".

Contudo, Rodotà (2008), alerta que há como excluir a possibilidade individuar uma determinada pessoa com base nesses dados, convertendo-se as informações em anônimas. Faz-se referência não a um sujeito determinado, mas ao grupo do qual faz parte. Em que pese a possibilidade de uma proteção da privacidade individual, todavia, não se mitiga a lógica da vigilância, que passa a ser aplicada ao grupo. Logo, não é cessada a afetação da "zona" da privacidade, pois as tecnologias da comunicação tendem a conflitar com "o direito de construir livremente a própria esfera privada, entendida como a autodeterminação informativa, como o poder de controlar a circulação das próprias informações". (RODOTÀ, 2008, p. 113).

Rodotà (2008) ainda admite que a vigilância não objetiva a obstrução ou desestímulo de comportamentos quando inserida dentro do contexto da lógica do mercado presente nas relações de consumo. Pelo contrário. O intuito é fazer com que os hábitos de consumo sejam quantitativamente reiterados. E nesta perspectiva da maximização da repetição de comportamentos de consumo, Rodotà (2008, p. 114) calcula o verdadeiro objetivo da vigilância, a classificação, pois "[...] a sociedade da vigilância revela-se, progressivamente, como sociedade da classificação".

A caracterização desta sociedade da classificação, na leitura de Rodotà (2008), é integrada pelas informações necessárias para se configurar as estratégias das regras de mercado e de consumo. É imprescindível, portanto, ter disponíveis a maior quantidade de dados dos destinatários de um produto, para individuar o alvo das campanhas publicitárias. Disso resulta uma produção, coleta e armazenamento de perfis individuais e de grupos para alimentar o cruzamento dos dados e gerar as mais diversas informações. Este raciocínio se aproxima da linha

desenvolvida por Bauman (2014b, 2008a), porque textualmente Rodotà (2008, p. 114) afirma que: "A sociedade se decompõe".

A decomposição da sociedade é questionada por Rodotà (2008) com as seguintes interrogações:

> Com quais efeitos? Uma adesão permanente às necessidades e aos gostos individuais, em uma perspectiva que exalta a soberania do consumidor? Ou a obrigação de entrar novamente em conformidade com parâmetros de normalidade estatística, sob pena de exclusão do mercado ou de acesso em condições particularmente onerosas? E portanto: um caminho para o reconhecimento das diversidades ou para a imposição de critérios de conformidade aos perfis prevalecentes? (RODOTÀ, 2008, p. 114).

As preocupações com esta decomposição ou fragmentação se avultam quando pensadas dentro do conflito entre as relações de mercado e a vida privada, pois "a classificação e a segmentação habitualmente determinam a seleção dos interesses comercialmente significativos, mais do que uma preocupação com cada aspecto da sociedade" (RODOTÀ, 2008, p. 114). A propagação da coleta de dados e informações pessoais avançam com maior especificidade e amplitude, deslocando "o eu de cada um de nós para lugares diversificados, indeterminados, intangíveis" (RODOTÀ, 2008, p. 125). E com isso se perde o direito à unicidade de cada pessoa: um indivíduo "multiplicado". Esta pulverização da pessoa em tantas "pessoas eletrônicas" fica a cargo da classificação impingida pelas regras de mercado e atende a interesses que induzem a coleta de informações.

A classificação, portanto, conduz à exclusão dos que não atendem aos interesses de uma pré-determinada moldura, alcançando efeitos que podem comprometer bens e serviços determinantes para a construção da personalidade e para a participação política. Com efeito, nesta confluência entre a premissa da classificação, regras de mercado/consumo e vida privada, Rodotà (2008, p. 114) observa que a tutela da diversidade será somente contemplada se em conformidade com as compatibilidades do mercado, é dizer, se adstrita ao que é classificado como critério do que é "normal", "que tende cada vez mais a coincidir com a conveniência econômica". Rodotà (2008) se preocupa, pode-se dizer, com uma problematização sociopolítica. Não se pode

acolher, sem ressalvas, o reconhecimento formal de um direito de acesso às redes ou de um direito a conhecer quem irá coletar ou conservar as informações provenientes da operação econômica. Tanto o direito de acesso, como o conhecimento prévio da episódica coleta de dados podem ter reduzidas suas projeções à mera ciência desta catalogação das informações, sem maiores repercussões.

O processo "seletivo" e classificatório pode agudizar a fragmentação da sociedade e se distanciar do sentido de comunidade. A estigma negativa desta "seleção" pode conduzir a distorções do processo formativo da personalidade. Tendo este contexto em vista, Rodotà (2008) requer uma extensão das garantias constitucionais para esta nova realidade, com o reconhecimento da legitimidade das escolhas dos que priorizam sua presença nas redes e a consideram uma instância decisiva para a construção de sua própria identidade. E neste ponto a concepção de anonimato de Rodotà (2008) tematiza (mas não se opõe) sobre outra ótica à evidenciada por Bauman (2014b).

Rodotà (2008) aposta que na comunicação eletrônica há de se dar espaço para a assunção de identidades, inclusive revestidas do anonimato. Isso porque para a configuração da liberdade existencial, deve-se admitir uma condição de aplicabilidade do livre desenvolvimento da personalidade, um direito já reconhecido em algumas Constituições democráticas, como a alemã e a italiana, e que no Brasil pode ser inferida da cláusula geral da dignidade da pessoa humana (art. 1º, III, CF-88). A preocupação com o anonimato de Rodotà (2008) ressalta o caráter contra-hegemônico de sua prefiguração, pois ao se assumir uma identidade diversa, refuta-se a adesão aos estereótipos predominantes e classificatórios preconcebidos pela regra estritamente de mercado. Isso porque a lógica da "seleção" é "paga" quando se amolda condicionamentos dos critérios de "normalidade". E esta ocorrência pode sublinhar as sujeições, pois "No mundo virtual não se encontraria a chantagem, apenas uma repetida servidão". (RODOTÀ, 2008, p. 118).

A concepção de anonimato, portanto, é entremeada pelas conjecturas não lineares das relações entre identidades reais e identidades virtuais. Com isso, Rodotà (2008) propõe uma a inclusão do anonimato em uma revisão do conceito de identidade, diverso do reducionismo biológico, para adentrar nas prospecções de construção incessante que as tecnologias da informação e da comunicação podem

fornecer. O argumento da inclusão do anonimato no conceito revisado de identidade leva em conta a modificação do contexto, do horizonte e do meio em que muitos constroem a identidade, ao ponto de Rodotà (2008, p. 119) questionar: "Se ontem foi possível dizer que o meio era a mensagem, hoje devemos dizer que a identidade é a máquina, que a identidade tende a se transferir inteira para o aparato tecnológico utilizado?".

Com esta pergunta, Rodotà (2008) pondera sobre a corporalidade e a sua extensão eletrônica, para meditar sobre as transformações do corpo e do seu destino, sob o pálio da realidade virtual. A multiplicidade da identidade pode ser edificada *diacronicamente* no desenvolvimento de várias intercorrências, assumindo-se diversos papéis e funções. E ainda pode ser assumida uma pluralidade de identidades, manifestadas *sincronicamente* no mesmo instante, graças à ubiquidade ou desterritorialização da rede. Rodotà (2008), portanto, quer fazer valer a característica do polimorfismo da identidade e insiste na sua flexibilidade, pois:

> Cada barreira de sexo, idade, profissão, pode ser superada. A variabilidade toma o lugar da estabilidade: o *eu* se torna múltiplo, fluido, passa a ser construído em interação contínua com as máquinas. E pode chegar ao ponto de assumir a identidade alheia: Eu sou o outro. Assim, navegando na Internet, cada um pode encontrar o próprio "duplo". Em todos os sentidos, a identidade se torna "nômade".
> [...]
> Múltipla e fluida, a identidade assume desta forma um caráter que acarreta consequências sociais e políticas de grande importância. Realmente, uma identidade continuamente enriquecida e lapidada pode ser mais dificilmente reconduzida a parâmetros de normalidade: e isso significa que deveria se tornar mais difícil, e menos aceitável, uma discriminação entre pessoas baseada em critérios *standard*, em perfis automatizados. (RODOTÀ, 2008, p. 120-121).

Esta aposta da revisão da identidade pelas tecnologias da informação e comunicação, elaborada por um dinamismo de gradações, legitimaria o direito à unicidade de cada pessoa e refutaria a estigmatização classificatória da sociedade que liga as identidades à consonância de uma maioria hipotética. A identidade, neste sentido, converte-se na medida de distância ou aproximação do outro sob duas

perspectivas, tanto se enfatizados os traços de reconhecimento recíproco, o que favorece a diversidade; como se realçados os elementos distintivos típicos, nos quais se pode contrapor os que estão em conflito. E é por estas razões que se postula que "a *virtualidade* deve então ser considerada com um aspecto da *realidade".* (RODOTÀ, 2008, p. 121).

Contudo, a realidade da virtualidade do anonimato, alerta Rodotà (2008), pode causar tensões. Isso porque a quem viola a privacidade alheia, permanecendo anônimo, pode tornar extremamente difícil o cabimento de contramedidas. Conjugam-se nesta disputa uma privacidade *ativa* contra uma privacidade *passiva*. É neste embate que foi e é necessária uma regulação para desenvolver uma série de princípios, com quais foram referenciados o direito de acesso e a preocupação de se relacionar a finalidade declarada e a coleta de dados (RODOTÀ, 2008). A partir desta necessidade, Rodotà (2008) agrega a promoção das *Privacy Enhancing Tecnologies* (*PET*), decorrentes do planejamento de sistemas que criam condições técnicas protetivas da privacidade, mas as vê com ressalvas.

Rodotà (2008) critica as premissas estritamente comerciais que configuram as proteções legislativas, as quais se contentam com os reflexos regulatórios dos instrumentos que coletam e tratam os dados, para salientar uma perspectiva mais "cidadã" do reforço de um direito à autodeterminação informativa. Isso porque é inegável uma interferência no poder de controle sobre as próprias informações, diante das fragmentações incitadas pelas coletas de dados. E a tutela "simplista" da privacidade, vista exclusivamente sob a ótica da resolução dos problemas do "empreendimento" que se faz com os dados coletados, pode resultar em uma "legitimação" jurídica e social das tecnologias de vigilância, sem levar em conta o uso completamente instrumental desta legitimidade. E a problematização não instrumental da tutela da privacidade no contexto das informações e dados pessoais, "[...] é justamente neste ponto que se localiza a fronteira entre a sociedade da informação e a sociedade da vigilância" (RODOTÀ, 2008, p. 126).

É por isso que um dos pontos de defesa da proteção de dados pessoais como direito fundamental é a sua reinvenção a partir de paradigmas de potencialidade sociopolítica, revestidos com o conteúdo da liberdade de desenvolvimento da própria personalidade, e não apenas

como instrumento protetivo atrelado estritamente às estratégias dos interesses de segurança e da lógica do mercado:

> Reiventar a proteção de dados constitui um processo constante que é indispensável não apenas para oferecer proteção adequada a um direito fundamental, mas também para impedir que novas sociedades se tornem sociedades de controle, vigilância e seleção social. (RODOTÀ, 2008, p. 21).

Rodotà (2008) rechaça, portanto, uma tutela da privacidade que se resuma ao jogo das transações do mercado ou aos limites da segurança, que subsuma o cidadão exclusivamente ao seu papel de consumidor, que visualiza as relações sociais somente com a lente do comércio eletrônico, convertendo a Internet em "um lugar asséptico, onde o consumidor, adulto ou criança, pode entrar como em um imenso *shopping center*, sem correr o risco de ser incomodado por qualquer coisa que possa afastá-lo da simples atividade de consumo." (RODOTÀ, p. 158). Por isso que, seguindo esta linha, não se pode superestimar as positivações protetivas da privacidade sem antes se averiguar se há elementos que distorcem a liberdade de escolha e o consentimento individual, pois há de se cotejá-las:

> em razão das assimetrias do poder ligadas à cultura, à renda, à concreta força no mercado. O processo de fortalecimento do poder individual, portanto, deve mover-se a partir da constatação da realidade: sem mecanismos capazes de depurá-la destas assimetrias, a manifestação do consentimento será formalmente livre, porém substancialmente estará vinculada às distorções do mercado. (RODOTÀ, 2008, p. 127).

Esta objeção aos condicionamentos impostos pelas regras exclusivas do mercado/consumo nas quais é dado consentimento individual é coerente com a formulação do fetichismo da subjetividade de Bauman (2014b, 2008b). Neste "novo" fetichismo, a privacidade seria um "novo" direito de propriedade sobre as informações pessoais, pois se compra e se vende "os símbolos empregados na construção da identidade", mercadorias viscerais para o "comércio" de informações pessoais. "Mudaria a própria natureza do direito à privacidade: de um direito fundamental da pessoa se transformaria em título a ser negociado no mercado" (RODOTÀ, 2008, p. 132).

Os condicionamentos do meio em que são feitas as relações intersubjetivas, a retórica do argumento do consentimento, as estratégias para a elaboração dos princípios e das regras jurídicas, indiscutivelmente tangenciam o monitoramento, o controle, a observação, a classificação, a checagem e a atenção sistemática aos dados pessoais no contexto da vigilância. E sobre estas inflexões, a releitura do pan-óptico feita por Bauman (2014b) auxilia na compreensão da sua hipótese pós-panóptica de análise. Estas digressões serão feitas no tópico a seguir.

3 REFLEXÕES PÓS-PANÓPTICAS SOBRE A VIGILÂNCIA: O SINÓPTICO E O BAN-ÓPTICO

Nas cartas em que formula a sua estrutura arquitetônica, Bentham (2013) indica algumas palavras que conduzem ao pensamento do projeto "panóptico" uma palavra baseada no grego, que significa "lugar de onde tudo se vê". Descreve que se tratava de um "novo modo de garantir o poder da mente sobre a mente, em um grau nunca antes demonstrado; e em um grau igualmente incomparável, para quem assim o desejar, de garantia contra o exagero" (BENTHAM, 2013, p. 80-81). A arquitetura projetada poderia ser aplicável a todos os estabelecimentos do destinatário das cartas (prisões perpétuas, prisões de confinamento, casas penitenciárias, casas de correção, casas de trabalho, manufaturas, hospícios, hospitais ou escolas), "num espaço não demasiadamente grande para que possa ser controlado ou dirigido a partir de edifícios, queira-se manter sob inspeção um certo número de pessoas". (BENTHAM, 2013, p.118-119).

Neste sentido, Bentham (2013) reputa como ideal que a cada momento do tempo os que inspecionam visualizem as pessoas a serem inspecionadas. Contudo, dada a impossibilidade deste fato (naquela época), é desejável que os inspecionados acreditem e pensem que estão nesta condição de visibilidade. Para este fito, o panóptico se vale de unidades espaciais que permitem a visualização ininterrupta e o reconhecimento imediato. A visibilidade, pois, é o ardil. Procura-se que a indução do "detento" à consciência de sua permanente visibilidade

resulte num funcionamento automático do poder, como efeito do panóptico (FOUCAULT, 2010)[4].

Sem embargo, se a visibilidade é um aspecto do panóptico, o outro é o poder inverificável. O "detento" deve ter a consciência de que é incessantemente espionado. Contudo, não deveria saber (verificar) se está sendo observado, apesar de certamente sempre poder sê-lo. Da torre central, portanto, pode ser ver tudo, sem nunca ser visto. Edifica-se a impossibilidade de se escapar da vigilância do outro, em razão constante observação. Este *dispositif* revela a automatização e a desindividualização do poder. (FOUCAUT, 2010).

Desnecessária, portanto, a força para impor a disciplina dos corpos, a fim de torná-los dóceis. A consciência da constante visibilidade sobre si (o "detento") direciona as ramificações do poder, fazendo-as funcionar espontaneamente como um primado de sua própria sujeição. O "laboratório do poder" que representa o panóptico, neste contexto, ainda que seja exógeno/externo, prescinde dos fardos físicos e corpóreos. O panóptico, segundo Foucault (2010), intensifica qualquer aparato de poder. Isso porque garante a economia em material, em pessoal e em tempo; o seu caráter preventivo, a sua continuidade de funcionamento e a sua automatização dos mecanismos afiançam a sua eficácia. É um modo, pois, de obtenção de poder. E esta perspectiva de poder é alentada pelo próprio Jeremy Bentham quando professa:

---

[4] Foucault (2010) explica a arquitetura do panóptico que atribui a Bentham consiste "[...] na periferia uma construção em anel; no centro, uma torre: esta é vazada de largas janelas que se abrem sobre a face interna do anel; a construção periférica é dividida em celas, cada uma atravessando toda a espessura da construção; elas têm duas janelas, uma para o interior, correspondendo às janelas da torre; outra, que dá para o exterior, permite que a luz atravesse a cela de lado a lado. Basta então colocar um vigia na torre central, e em cada cela trancar um louco, um doente, um condenado, um operário ou um escolar. Pelo efeito da contraluz, pode-se perceber da torre, recortando-se exatamente sobre a claridade, as pequenas silhuetas cativas nas celas da periferia. Tantas jaulas, tantos pequenos teatros, em que cada ator está sozinho, perfeitamente individualizado e constantemente visível. O *dispositif* panóptico organiza unidades espaciais que permitem ver sem parar e reconhecer imediatamente. Em suma, o princípio da masmorra é invertido; ou antes, de suas três funções – trancar, privar de luz e esconder – só se conserva a primeira e suprimem-se as outras duas. A plena luz e olhar de um vigia captam melhor que a sombra, que finalmente protegia. A visibilidade é uma armadilha" (FOUCAULT, 2010, p. 190).

> A moral reformada; a saúde preservada; a indústria revigorada; a instrução difundida; os encargos públicos aliviados; a economia assentada, como deve ser, sobre uma rocha; o nó górdio da Lei sobre os Pobres não cortado, mas desfeito – tudo por uma simples ideia de arquitetura! (BENTHAM, 2013, 77-79).

Foucault (2010) comenta que o diagrama panóptico, sem a perda de seus pilares, tem como destino a difusão no corpo social, generalizando-se, constituindo-se um princípio de uma nova "anatomia política", não adstritas às relações de soberania, mas incluídas as relações de disciplina. Foucault (2010) separa a disciplina-bloco; a instituição fechada, vocacionada para as atribuições negativas, como o rompimento das comunicações, a suspensão do tempo, para fazer o mal; da disciplina-mecanismo do panoptismo, que funcionalmente melhora o exercício do poder por torná-lo mais rápido, leve e eficaz. Por esse motivo "[...] forma-se então uma política das coerções que são um trabalho sobre o corpo, uma manipulação calculada de seus elementos, de seus gestos, de seus comportamentos". (FOUCAUT, 2010, p. 133). Avança-se da disciplina-bloco para a disciplina-mecanismo, de uma disciplina de exceção para uma disciplina de vigilância generalizada incutida no corpo social, para a conformação, por meio do panoptismo, da sociedade disciplinar.

A disciplina representa um tipo de poder e uma maneira de exercê-lo, que conta com instrumentos, técnicas, procedimentos que a elevam a uma tecnologia do poder. Ao se generalizar esta tecnologia de poder, alimentada pelo programa do panóptico, Foucault (2010) caracteriza a nossa sociedade como de vigilância. Elenca, para tanto, os processos históricos e os pressupostos econômicos, jurídico-políticos e científicos para esta caraterização (FOUCAUT, 2010).

Em *Vigilância Líquida* (2014b), Bauman e David Lyon refletem a vigilância sobre outros contextos históricos dos que os examinados por Foucault (2010). E por isso se reportam a uma perspectiva pós-panóptica para analisar a vigilância. Esta perspectiva não abandona a rica construção do "laboratório do poder" do panoptismo, mas tenta nela agregar elementos diferenciadores.

Neste sentido, Lyon se reporta a Didier Bigo que propôs que o "ban-óptico". Este programa indica como as tecnologias de elaboração de perfis são usadas para determinar quem será colocado sob vigilância

específica. Parte de uma construção teórica da nova insegurança global. O mecanismo de vigilância e de controle que trabalham a distância para monitorar e controlar conectam com o que Foucault (2010) chamou de *dispositif*. Com a vigilância, com a seleção e com a classificação, criam-se categorias de pessoas excluídas, com o uso de base de dados em rede.

Didier Bigo, segundo Lyon, afirma que no modelo ban-óptico não há uma manifestação centralizada como no panóptico, mas que o *dispositif* é algo fragmentado e heterogêneo. Opera por meio do Estado e das grandes corporações. Analisa-se o discurso (de risco, de ameaça, dos inimigos internos, de segurança), as instituições, as estruturas arquitetônicas (de centros de detenção a terminais de passageiros em aeroportos), legislações e atos administrativos. O objetivo do diagrama do ban-óptico é esboçar o perfil das minorias "indesejadas". Triparte as características do ban-óptico em:

> o poder excepcional em sociedades liberais (estados de emergência que se tornam rotineiros), traçar perfis (excluir certos grupos, categorias de pessoas excluídas de forma proativa em função de seu potencial comportamento futuro) e normalizar grupos não excluídos (segundo a crença no livre movimento de bens, capital, informações e pessoas). (BAUMAN, 2014b, p. 53).

Ainda, Bauman e David Lyon (2014b) se referem ao "sinóptico", de Thomas Mathiesen. O sinóptico contrasta "poucos vigiando muitos" do pan-óptico à mídia atual, em que "muitos vigiam poucos". Isso sugere como o pan-óptico pode se deparar com um aliado nos atuais meios de comunicação no que se refere à vigilância. O argumento de Mathiesen, que utiliza a modernidade líquida, é que os efeitos atuais nas sociedades não podem ser entendidos separadamente do sinóptico, no mínimo porque ajudam a moldar os efeitos deste.

A vigilância líquida, pós-panóptica é baseada no processamento de dados e mediada por informações dentro do contexto das tecnologias de comunicação. Permitem uma nova transparência, voltada para o monitoramento, para o controle, para a observação, para a classificação, para a checagem dos usuários e "venda" de dados pessoais; para estabelecer uma servidão do tipo <faça você mesmo>. Este tipo de servidão é extraído do paralelo líquido moderno do *Discurso sobre a*

servidão voluntária (2017), escrito em 1549 por Étienne de la Boétie e publicado originalmente na França em 1576.

De la Boétie (2017) problematiza a dominação e o poder em contraste com a liberdade e a autonomia. Sua análise é direcionada para as tiranias de sua época. Alerta que não é preciso combater tampouco derrotar um tirano, pois um país que não consente com a servidão, não lhe dará nada:

> [...] São, portanto, os próprios povos que se deixam ou, ainda, se fazem maltratar, pois ao pararem de servir estariam livres; é o povo que se subjuga, que corta a própria garganta, que, podendo escolher entre servir ou ser livre, abandona a liberdade e toma o jugo, que consente com seu infortúnio e até mesmo o busca. [...]. (DE LA BOÉTIE, 2017, p. 39).

Neste sentido, De la Boétie (2017) admite que a servidão é voluntária, pois a liberdade é um direito natural e só é retirada pelo próprio consentimento de quem aceita a servidão. Pondera que o seres nascem não só com a liberdade, mas também com o desejo de defendê-la. Exemplifica que o elefante, o cavalo, o boi, os pássaros ficam irresignados e se manifestam quando estão diante de uma ameaça de sua liberdade. Por isso, o argumento do consentimento, nesta literatura, é o pressuposto da servidão voluntária, pois "[...] Como é possível que tenha algum poder sobre vós senão por meio de vosso consentimento? Como ousaria atacar-vos sem vossa cooperação?" (DE LA BOÉTIE, 2017, p. 42). E arremata que:

> [...] se todos os seres sencientes rapidamente constatam o mal da sujeição e a necessidade de liberdade, e se nem as bestas, mesmo sendo criadas a serviço dos homens, conseguem se acostumar a servir sem manifestar desejo oposto, que terrível desencontro foi esse que tanto desnaturou o homem, o único realmente nascido para viver em liberdade, e o fez perder a lembrança de seu estado original e o desejo de resgatá-lo? (DE LA BOÉTIE, 2017, p. 46-47).

É certo que estes questionamentos são feitos em um tempo e em um espaço diferentes dos atuais. Também é certo que qualquer das respostas a De la Boétie (2017) não podem desconsiderar a coerção corpórea e a força física, imperantes naquela quadra histórica. Nada

obstante, não é imprópria, pelo próprio arrazoado do texto, a analogia da servidão voluntária com o fetichismo da subjetividade, com a voluntariedade da servidão do <faça você mesmo> e com a retórica do argumento do consentimento.

Bauman (2014b), inclui a tentação e a sedução como as chaves da eficiência em produzir um comportamento desejável. E por isso defende uma hipótese pós-panóptica de vigilância. Esta hipótese parte da consideração de que a vigilância arquitetada pelo pan-óptico direcionava a submissão/sujeição pela eliminação da escolha. A consciência da constante visibilidade sobre si e a inverificabilidade do poder eliminam as escolhas, disciplinam dos corpos, a fim de torná-los dóceis. Por isto, a proposta panóptica tende a ser excludente, no contexto de uma "imobilidade" e de um "aprisionamento".

A pós-panóptica se diferencia desta pois é inclusiva. Permite-se a escolha. Na modernidade líquida, a leitura do pós-panóptico é feita a partir da "mobilidade" e da "liberdade de escolha". Contudo, a vigilância empregada pelo mercado/consumo possui como premissa a manipulação da escolha pela sedução, não pela coerção:

> A cooperação não apenas voluntária, mas entusiástica, dos manipulados é o principal recurso empregado pelos sinópticos dos mercados de consumo. [...] parece um atributo geral da forma de vida moderna (conhecida por sua obsessão por diferenciação, classificação e arquivos), agora amplamente reempregado para uma estratégia em tudo alterada no curso da transição para a sociedade líquida moderna de consumidores. Reempregada em nome da inclusão da <livre escolha> na estratégia de marketing, ou, mais precisamente, de tornar voluntária a servidão e fazer com que a submissão seja vivenciada como um avanço da liberdade e um testemunho da autonomia de quem escolhe (já descrevi esse processo em outro texto, chamando-o de <fetichismo da subjetividade>). (BAUMAN, 2014b, p. 109-110).

Com o fetichismo da subjetividade, a automatização do controle e da dominação faz com que a vigilância líquida traslade os deveres gerenciais para os próprios gerenciados, transforma-os de passivos para ativos, isto é, "de custos para ganhos – terceirizando essa tarefa para aqueles que se encontram na extremidade receptora da operação." (BAUMAN, 2014b, p. 114). Para Bauman (2014b), Focault caracteriza o panóptico como "arquimetáfora do poder moderno", ao revelar a

disciplina-mecanismo panóptica, ou de "treinamento da alma", para produzir "detentos" bem-ordenados. No panóptico, os prisioneiros estavam sob vigilância constante e por isso não se moviam; tinham de permanecer o tempo todo nos lugares designados porque não sabiam, nem tinham como saber, onde estariam os guardas. Com a "modernidade líquida", a rigidez destes movimentos dos prisioneiros "se dissolveu", de tal forma que a vigilância se configura como pós-panótica (BAUMAN, 2014b).

CONCLUSÕES

O objetivo deste texto foi examinar, por meio de uma metodologia analítica as conexões entre a obra "A vida na Sociedade da Vigilância" de Rodotà e "Vigilância Líquida" de Zygmunt Bauman, acrescida da discussão de outros autores sobre a sociedade de consumo, bem como de suas especificidades. O texto foi organizado em tópicos que discutiram o que cada autor estima como pressuposto para configurar o conceito de vigilância. Em seguida, foram cotejados estes conceitos no marco da hipótese pós-panóptica defendida por Bauman. As principais são as listadas as seguir.

Bauman adverte que a vigilância contemporânea, com monitoramento, o controle, a observação, a classificação, a checagem e a "venda" (consumo) de dados, conseguiu que os indivíduos, com a servidão do <faça você mesmo>, sejam simultaneamente promotores de produtos e os produtos que promovem. Os "usuários" são, ao mesmo tempo, as mercadorias e os agentes de marketing, os produtos e os vendedores itinerantes, para que augurem uma visibilidade e, porventura, <valor social> e/ou autoestima.

Para Bauman uma das características do avanço da sociedade consumista foi a passagem da produção direcionada para a demanda existente, de satisfação de necessidades; para a demanda voltada para a produção existente (a sua criação) "por meio de tentação, sedução e estímulo do desejo assim despertado". Busca-se, portanto, o direcionamento de ofertas a pessoas ou categorias de pessoas já previamente prontas para aceitá-las, entusiasmadas. A dispendiosa estratégia de marketing de despertar desejos foi transferida para os potenciais consumidores. E é nesta nova perspectiva que Bauman insere

a tecnologia de vigilância, do controle, da observação, da classificação, da checagem e da atenção sistemática aos dados dos usuários, para comercializá-los na lógica do consumo.

A vigilância contemporânea logrou; com o monitoramento, o controle, a observação, a classificação, a checagem dos usuários e "venda" de dados pessoais; estabelecer uma servidão do tipo <faça você mesmo>, em que se consente, por vontade própria, trabalhar a serviço de uma mesma realidade. O estratagema panóptico (você nunca vai saber quando é observado, nunca imagine que não está sendo espionado) é implantado, aos poucos, em escala global. Contudo, altera-se o <Nunca estou sozinho> para o esperançoso <Nunca mais vou ficar sozinho> (abandonado, ignorado, desprezado, excluído), o medo da exposição é intercambiado pela alegria de ser notado. A visibilidade, antes uma ameaça, foi reclassificada para uma tentação, para o desejo de ser visto. A exposição se converte na prova de reconhecimento social.

A vigilância líquida, pós-panóptica é baseada no processamento de dados e mediada por informações dentro do contexto das tecnologias de comunicação. Permitem uma nova transparência, voltada para o monitoramento, o controle, a observação, a classificação, a checagem dos usuários e "venda" de dados pessoais; estabelecer uma servidão do tipo <faça você mesmo>.

Os condicionamentos do meio em que são feitas as relações intersubjetivas, a retórica do argumento do consentimento, as estratégias para a elaboração dos princípios e das regras jurídicas, indiscutivelmente tangenciam o monitoramento, o controle, a observação, a classificação, a checagem e a atenção sistemática aos dados pessoais no contexto da vigilância.

Rodotà critica as premissas estritamente comerciais que configuram as proteções legislativas, as quais se contentam com os reflexos regulatórios dos instrumentos que coletam e tratam os dados, para salientar uma perspectiva mais "cidadã" do reforço de um direito à autodeterminação informativa. Isso porque é inegável uma interferência no poder de controle sobre as próprias informações, diante das fragmentações incitadas pelas coletas de dados. E a tutela "simplista" da privacidade, vista exclusivamente sob a ótica da resolução dos problemas do "empreendimento" que se faz com os dados coletados, pode resultar em uma "legitimação" jurídica e social das tecnologias de vigilância, sem

levar em conta o uso completamente instrumental desta legitimidade. E a problematização não instrumental da tutela da privacidade no contexto das informações e dados pessoais delimita a fronteira entre a sociedade da informação e a sociedade da vigilância.

É por isso que um dos pontos de defesa da proteção de dados pessoais como direito fundamental é a sua reinvenção a partir de paradigmas de potencialidade sociopolítica, revestidos com o conteúdo da liberdade de desenvolvimento da própria personalidade, e não apenas como instrumento protetivo atrelado estritamente às estratégias dos interesses de segurança e da lógica do mercado.

Com o fetichismo da subjetividade, a automatização do controle e da dominação faz com que a vigilância líquida traslade os deveres gerenciais para os próprios gerenciados, transforma-os de passivos para ativos, isto é, "de custos para ganhos – terceirizando essa tarefa para aqueles que se encontram na extremidade receptora da operação". Para Bauman, Focault caracteriza o panóptico como "arquimetáfora do poder moderno", ao revelar a disciplina-mecanismo panóptica, ou de "treinamento da alma", para produzir "detentos" bem-ordenados. No panóptico, os prisioneiros estavam sob vigilância constante e por isso não se moviam; tinham de permanecer o tempo todo nos lugares designados porque não sabiam, nem tinham como saber, onde estariam os guardas. Com a "modernidade líquida", a rigidez destes movimentos dos prisioneiros "se dissolveu", de tal forma que a vigilância se configura como pós-panótica. A pós-panóptica se diferencia da anterior pois é inclusiva. Permite-se a escolha. Na modernidade líquida, a leitura do pós-panóptico é feita a partir da "mobilidade" e da "liberdade de escolha". Contudo, a vigilância empregada pelo mercado/consumo possui como premissa a manipulação da escolha pela sedução, não pela coerção.

Como contributo principal desta reflexão, tem-se portanto o argumento de que na modernidade, a vigência do panóptico estava pautada na imobilidade e no aprisionamento, enquanto que na modernidade líquida, a hipótese do pós-panóptico é sustentada com a mobilidade, com o monitoramento à distância e com a servidão voluntária.

REFERÊNCIAS

AGUERO, R. A. **A construção do discurso sobre o trabalho infantil**: mídia, imagens e poder. Dissertação (Mestrado em Letras) – Universidade Federal do Mato Grosso do Sul – Campus Três Lagoas/MS, 2008. [Dissertação de Mestrado não publicada].

ALMEIDA, Milton José de**. Imagens e Sons:** a nova cultura oral. São Paulo: CORTEZ, 2001.

AUGÉ, Marc. **Não Lugares:** uma introdução à antropologia da supermodernidade. SP/CAMPINAS: Papirus, 1990.

BAUDRILLARD, Jean. **A sociedade de consumo.** Lisboa: Edições 70, 1981.

BAUMAN, Zygmunt. **Modernidade Líquida.** [E-book]. Rio de Janeiro: Zahar, 2001.

BAUMAN, Z. **A sociedade individualizada**: vidas contadas e histórias vividas. [E-book]. Rio de Janeiro: Zahar, 2008.

BAUMAN, Zygmunt. **Vida para consumo**: a transformação das pessoas em mercadoria. Rio de Janeiro: Zahar, 2008.

BAUMAN, Zygmunt. **44 cartas do mundo líquido moderno**. Rio de Janeiro: Zahar, 2011.

BAUMAN, Zygmunt. **Cegueira moral:** a perda da sensibilidade na Modernidade Líquida**.** [E-book]. Rio de Janeiro: Zahar, 2014.

BAUMAN, Zygmunt. **Vigilância Líquida**. [E-book]. Zahar: Rio de Janeiro, 2014.

BENTHAM, Jeremy. **O panóptico.** Organização de Tomaz Tadeu. Traduções de Guacira Lopes Louro, M. D. Magno e Tomaz Tadeu. [E-book]. São Paulo: Autêntica, 2013.

BERMAN, Marshall. **Tudo que é sólido desmancha no ar**: a aventura da modernidade. São Paulo: Companhia das letras, 1986.

BOURDIEU, Pierre. **A distinça o:** cri tica social do julgamento. São Paulo: EDUSP, 2007.

CANEVACCI, Massimo. **A cidade polifônica**. SP: Studio Nobel, 1995.

DELEUZE, G. *Post-Scriptum* sobre as Sociedades de Controle. In: **Conversações**. 2. Ed. São Paulo: Editora 34, 2010.

FEATHERSTONE, Mike. **Cultura de consumo e Pós - Modernismo**. São Paulo: Studio Nobel,1993.

FOUCAULT, M. **Vigiar e punir:** nascimento da prisão. 38. ed. Petrópolis: Vozes, 2010.

GERGEN, Mary; GERGEN, Kenneth, J. **Social Contruction:** a Reader. NYC: Sage Publication, 2003.

GIDDENS, Anthony. **As conseqüências da Modernidade**. São Paulo: Unesp,1991.

GUATTARI, F. **Caosmose:** um novo paradigma estético. São Paulo: Editora 34, 1992.

GUATTARI, F.; ROLNIK, S. **Micropolítica:** cartografias do desejo. Petrópolis: Vozes, 1996.

JAMENSON, Frederic. **Pós - Modernismo:** a lógica cultural do capitalismo tardio. São Paulo: Ática,1996.

JOHNSON, S. **Cultura da interface**: Como o computador transforma nossa maneira de criar e comunicar. Rio de Janeiro: Jorge Zahar, 2001.

LA BOÉTIE, Étienne de. **Discurso sobre a servidão voluntária**. São Paulo: Edipro, 2017.

MACHADO, Arlindo. **Máquina e Imaginário**. SP:EDUSP, 1993.

MANOVICH, Lev. **El lenguaje de los nuevos médios de comunicación**: la imagen en la era digital. Buenos Aires: Paidós comunicación, 2005.

ORTIZ, Renato. **A moderna Tradição Brasileira**. SP: Brasiliense, 1987.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SANTAELLA, L. **Cultura das mídias.** SP: Experimento, 1996.

SANTAELLA, Lúcia. **Linguagens líquidas na era da Mobilidade**. SP: Paulus, 2007

SARLO, Beatriz. **Cenas da vida pós-moderna**. Rio de Janeiro: UFRJ, 1997.

COOPERAÇÃO ENTRE ESTADOS TOTALITÁRIOS E CORPORAÇÕES: O USO DA SEGMENTAÇÃO DE DADOS E *PROFILING* PARA VIOLAÇÃO DE DIREITOS HUMANOS

Cinthia Obladen de Almendra Freitas[1]
Danielle Anne Pamplona[2]

1. Introdução

Há muito os Estados deixaram de ser os únicos violadores de direitos humanos. O esforço internacional no segundo pós-guerra para reunir os Estados no compromisso de proteger um rol de direitos provou-se insuficiente na medida em que novos atores aparecem no cenário internacional.

Nas jurisdições domésticas, os Estados têm o compromisso de prevenir e remediar as violações. Todavia, nem sempre isso é possível, e um dos motivos é que muitos Estados devem, no desempenho de sua função de proteção de seus cidadãos, enfrentar grandes oponentes. As grandes corporações são assim denominadas porque muitas vezes representam, financeiramente, mais do que o PIB de um Estado, e o desenvolvimento de sua atividade afeta positivamente a geração de empregos e o recolhimento de tributos de várias nações. Diante deste cenário, são vários os casos em que ocorrem violações de direitos humanos sem a ação estatal, mas sim, pelas 'mãos' de corporações. Não há um rol específico de direitos que sejam passíveis de violações por corporações, ao contrário, elas podem ser responsáveis pela violação de quaisquer dos direitos humanos internacionalmente reconhecidos. É possível, no entanto, que corporações de um setor específico identifiquem quais os direitos com maior possibilidade de serem

[1]Doutora em Informática pela Pontifícia Universidade Católica do Paraná (2001). Professora Titular da PUCPR para o curso de Direito (Módulo Temático: Perícias e Laudos Técnicos; Fraudes e Crimes por Computador). Professora Permanente do Programa de Pós-Graduação em Direito (PPGD) da mesma instituição. e-mail: cinthia@ppgia.pucpr.br

[2] Doutora em Direito pela UFPR – Universidade Federal do Paraná. Visiting Scholar na American University, Washington, DC (2015/2016); Professora Permanente do Programa de Pós-Graduação em Direito (PPGD) da PUCPR. Coordenadora da Clínica de Direitos Humanos do PPGD/PUCPR. E-mail: danielle.pamplona@pucpr.br.

afetados por sua atividade, assim, por exemplo, é possível afirmar que o setor de vestuários tem um potencial maior para violar direito à não escravidão ou servidão ou o setor extrativista, direito à integridade pessoal.

Mas, para além da possibilidade de que as corporações contratem ou deixem contratar, em sua cadeia produtiva, empregados em condições análogas à de escravos, ou mão de obra infantil, ou de que as corporações provoquem deslocamentos humanos, ou violações do direito à integridade pessoal, há também, a possibilidade de que elas atuem como cumplices do Estado para a ocorrência de violações.

É desta hipótese especifica que trata este texto. A intenção, aqui, é descortinar a hipótese em que corporações do setor de tecnologia e informação auxiliam Estados totalitários e sua atuação apresenta, como consequência, violações de direitos humanos. Para tanto, explora-se no que consiste a atividade destas corporações que podem ser utilizadas em benefício de Estados descompromissados com alguns direitos humanos, para então, demonstrar que direito é violado e em que extensão.

2. Segmentação de dados e *profiling*

Na visão de Schwab (2016) vive-se a "Quarta Revolução Industrial" sustentada pelas seguintes características: velocidade, amplitude e profundidade e, por último, impacto sistêmico. O autor explica que as mudanças estão ocorrendo em um ritmo exponencial e não linear, como tradicionalmente se busca descrever e enteder a tecnologia. Além disto, a combinação de várias tecnologias (multiplataformas, multitarefas, entre outros) e a tranformação de sistemas inteiros (desde países até empresas) "não está modificando apenas o 'o que' e o 'como' fazemos as coisas, mas também 'quem' somos" (SCHWAB, 2016, p. 13).

É neste contexto de transformação que o aspectos ligados ao tratamento de dados passa a assumir vital importância desde a esfera governamental até o usuário comum da Internet. Vive-se os 3 V's de Kitchin (2014, p. 68): volume, velocidade e variedade de tipos de dados, sendo os conjuntos de dados frequentemente referenciados temporal e espacialmente. Estas características configuram o que se entende por *Big Data* (KITCHIN, 2014).

Considerando o contexto do uso da Internet e acesso à informação em estados totalitários, apresenta-se e discute-se a segmentação de dados e a caracterização de perfil (*profiling*) por meio da aplicação de técnicas de Mineração de Dados em *Big Data*.

2.1 Segmentação de dados

Pariser (2012, p. 14) explica que a bolha informacional surge da junção dos mecanismos de busca e seus filtros com os mecanismos de previsão, os quais "criam e refinam constantemente uma teoria sobre quem somos e sobre o que vamos fazer ou desejar a seguir". Estes mecanismos "criam um universo de informações exclusivo para cada um de nós – o que passei a chamar de bolhas dos filtros – que altera constantemente o modo como nos deparamos com ideias e informações." Neste contexto, a bolha informacional apresenta aos usuários da Internet três dinâmicas, pontuadas por Pariser (2012, p. 14-15), a saber:

1) 1ª. Dinâmica: aponta que "estamos sozinhos na bolha", ou seja, mesmo compartilhando interesses comuns, os usuários sofrem a ação de uma força centrífuga, de dentro para fora, de modo que as bolhas se afastam uma das outras quando analisadas em modelo global;
2) 2ª. Dinâmica: indica que "a bolha é invisível". Pariser (2012) explica que não se pode escolher os critérios utilizados pelos mecanismos de busca e pelos filtros, mas o usuário intui que as informações a ele apresentadas são "imparciais, objetivas e verdadeiras". O autor afirma "que não são". Na verdade, "quando vemos de dentro da bolha, é quase impossível conhecer seu grau de imparcialidade" (PARISER, 2012, p. 15). Este grau de imparcialidade é, portanto, não definido, não conhecido e não percebido pelo usuário;
3) 3ª. Dinâmica, por sua vez, mostra que "não optamos por entrar na bolha", isso porque cada usuário é uma bolha. Os filtros personalizados são colocados a serviço do usuário sem que ele esteja atento para isto e, "por serem a base dos

> lucros dos sites que os utilizam, será cada vez mais difícil evitá-los" (PARISER, 2012, p. 15).

Estas dinâmicas, tal qual explicado por Pariser (2012), vão até os usuários criando um "... lugar confortável, povoado por nossas pessoas, coisas e ideias preferidas." Nasce assim o conceito de segmentação de dados que estrutura a formação do conceito de informação fragmentada por meio da oferta de informações direcionadas que podem ser controladas em casos de estados totalitários. Neste contexto, a segmentação de dados ocorre com o interesse de 'segmentar' o que pode ou deve circular as redes e, ainda, fragmentar a informação de modo a não se ter o todo, mas somente as partes da informação que pode ou deve circular as redes.

A informação fragmentada está diretamente ligada às características da Internet, as quais de acordo com Drake *et al*. (2016) fornecem um cenário composto pelas noções de alcance global com integridade e acessibilidade universal, possibilitando inovação sem permissão. Assim, a informação fragmentada é resultado da aplicação de sistemas de informação dispersos e heterogêneos, que estão sendo projetados de forma independente por diferentes empresas, a fim de aperfeiçoar individualmente a informação desejada por cada um dos usuários a partir de implementação de processos específicos com base no conjunto de dados de cada usuário. Eis o interesse dos estados totalitários, tratar não cada usuário, mas a nação como um grande usuário.

Tem-se por conjunto de dados tudo aquilo que os sistemas possam capturar sobre um determinado usuário, seus amigos, preferências, buscas, lugares, entre outros. Isto é possível, uma vez que a característica de alcance global com integridade possibilita que a informação seja recebida em qualquer ponto de conexão à Internet, ou seja, onde quer que o interessado se conecte à Internet tanto para acesso quanto para alimentar com dados os sistemas e aplicativos utilizados. Eis o alcance global com integridade e acessibilidade universal na ponta dos dedos dos usuários da Internet e, também, dos Estados.

Todas estas facilidades permitem inovação sem permissão, por meio da qual qualquer pessoa ou organização pode criar um novo serviço e disponibilizá-lo na Internet, sem necessidade de permissão

especial. Os autores questionam: "... considere o Facebook - se houvesse uma placa de aprovação de negócios para novos serviços de Internet, o Facebook teria sido possível avaliar corretamente o potencial do Facebook e o Facebook seria aprovado para uso?" (DRAKE *et al*., 2016, p. 11). Na China, o Facebook é proibido e desde 1994 quando a China se inseriu na rede mundial de computadores diversos sítios eletrônicos ou são proibidos ou foram totalmente banidos, podendo-se citar ainda: Google, YouTube, Twitter, Wikipedia, LinkedIn e DropBox (MACEDO, 2016).

Drake *et al*. (2016, p. 03) discutem tanto a fragmentação da Internet quanto a fragmentação na Internet, entendendo diferentemente cada uma destas categorias. Fragmentação da Internet ou a fragmentação advinda das infraestruturas físicas e lógicas que suportam a Internet em si. E, fragmentação na Internet ou a fragmentação que ocorre no ciberespaço e nas transações efetivadas por meio da Internet.

Levando em consideração estas categorias de fragmentação, Drake *et al*. (2016, p. 07) explicam que a fragmentação pode, inicialmente, referir-se à disseminação da censura, bloqueio, filtragem e outras limitações de acesso por governos e Estados, bem como à plataformas proprietárias e modelos de negócios que, em certa medida, impedem os usuários finais de criar, distribuir e acessar livremente informação. Mas, na verdade, a fragmentação a que os autores se referem é mais ampla do que isto, visto que a Internet não capta, por si só, como as pessoas usam e experimentam a tecnologia para construir formações sociais digitais e engajar-se em informações, comunicações e transações comerciais ou, até mesmo, os tipos de forças políticas e econômicas que influenciam as pessoas a desenvolver algo na Internet (DRAKE *et al*., 2016, p. 10).

Neste cenário de fragmentação, Drake *et al*. (2016, p. 40) discutem a privacidade e a proteção de dados no que tange às informações de identificação pessoal transmitidas para além das fronteiras territoriais ou geográficas, tornando o tema proteção de dados uma preocupação mundial.

A Internet fragmentada também possibilita e, ao mesmo tempo, exige requisitos de localização de dados (DRAKE *et al*., 2016, p. 41). Tudo que o usuário faz está diretamente associado ao local, ou seja, onde aquela imagem foi capturada ou onde um determinado usuário fez uma

consulta sobre um determinado produto, se em casa, no trabalho ou na rua. Para Drake *et al*. (2016, p. 41) a localização de dados é uma construção multidimensional, de modo que possam ser estudadas leis que limitam o armazenamento, o movimento e/ou o processamento de dados, sem deixar de levar em consideração o país da empresa de incorporação ou dos principais sites de operações e gestão dos dados e informações. Nos estados totalitários saber quem faz, o que faz e onde faz eleva os níveis de controle e vigilância.

Entende-se, portanto, que as bolhas informacionais estão associadas à informação fragmentada, uma vez que o usuário nunca terá em mãos a real totalidade de dados e informações disponíveis via Internet, mas sim o que lhe cabe em sua bolha única e personalizada. O maior risco está nos estados totalitários criarem e estabelecerem a bolha informacional como nação, fragmentando a informação a ponto de segmentar os dados dos usuários para controle e vigilância do que tais usuários realizam na Internet.

2.2 Caracterização de Perfil (*profiling*)

A segmentação de dados pode ainda atingir os usuários por meio da aplicação de técnicas de tratamento de dados, a exemplo da caracterização de perfil (*profiling*). Talvez o termo mais adequado em português seja perfilagem ou perfilamento, mas o que se percebe, mesmo nos artigos científicos, é o emprego da palavra inglesa. Assim, a caracterização de perfil refere-se aos métodos e técnicas computacionais aplicados aos dados pessoais ou não dos usuários. E, em tempos de *Big Data*, dados não faltam para serem processados.

As técnicas de perfilamento têm como objetivo determinar o que é relevante dentro de um determinado contexto, por exemplo, quem pode estar interessado em um determinado produto. Além disto, estas técnicas auxiliam na representatividade estatística, ou seja, na determinação da qualidade de uma amostra constituída de modo a corresponder à população no seio da qual ela é escolhida. Ou seja, busca-se generalizar a partir de uma amostra de indivíduos e dos seus respectivos interesses. Por exemplo, se um determinado grupo de pessoas está interessado em um determinado produto, outros grupos de

pessoas ligados, conhecidos ou relacionados ao primeiro grupo também pode vir a se interessar por este mesmo produto.

Muitas são as definições de perfilamento, mas Ferraris *et al.* (2003, p. 06) apresentam definições relevantes ao capítulo aqui proposto: "*the act or process of extrapolating information about a person based on known traits or tendencies, e.g. consumer profiling*" ou "*the act of suspecting or targeting a person on the basis of observed characteristics or behaviour, e.g. racial profiling*". Assim, Ferraris *et al*. (2003, p. 06) inferem que "*profiling is a process of construction of a series of information (a profile), which is then applied to something or someone (individual or group) by techniques of data elaboration*".

De acordo com Hildebrandt, (2009, p. 243) *profiling* pode ser definido como uma nova maneira de conhecimento que torna visível os padrões que são invisíveis ao olho humano, de modo que "*the invisibility of the patterns become visible to the profiler and the inability to anticipate the consequences of the application of profiles derived from other people's data clearly rule out informed consent*".

Na sociedade informacional e tecnológica em que se vive determinar o que é ou não relevante para os indivíduos é tão importante que Pariser (2012, p. 16) menciona que a "tarefa de examinar essa torrente cada vez mais ampla em busca das partes realmente importantes, ou apenas relevantes, já exige dedicação em tempo integral", de modo que "somos cada vez mais incapazes de dar conta de tanta informação". Portanto, métodos e técnicas de tratamento de dados, independentemente de que dados sejam, tem sido aplicados pelos mais variados sistemas, serviços, empresas, governos e Estados.

Como retratado por Duhigg (2012, p.81-82), a Target, gigante rede de lojas de departamento dos Estados Unidos, atribuiu um número único a cada um de seus clientes e passou a armazenar dados relativos às suas compras, identificando assim seus produtos preferidos, hábitos de consumo, valor médio de gastos, uso ou não de cupons e cartão fidelidade. Juntamente com dados pessoais de cadastro que identificavam dentre outras informações, sexo, idade, profissão e local de moradia, contratou estatísticos que, utilizando ferramentas computacionais, analisaram estes dados para extrair conhecimento relevante, estabelecendo padrões de consumo de cada cliente, permitindo assim alavancar suas vendas.

Para tal, podem ser aplicados diferentes algoritmos tanto para descobrir padrões quanto para determinar a correlação entre conjuntos de dados, de modo a estabelecer um perfil, visto que tais padrões e correlações permitem identificar ou representar pessoas ou grupos de pessoas. Eis o risco da discriminação, segregação ou outra forma de violência contra a pessoa, seja esta violência simbólica (BOURDIEU, 1994) ou não, incluindo-se a discriminação baseada em dados à saúde, opção sexual, religiosa, filosófica, moral, política, racial entre outras. Os dados que descrevem tais atributos de uma pessoa são denominados de dados sensíveis, visto que se revestem de especial sensibilidade. Porém, tal qual PINHEIRO (2015, p. 648) "a classificação de certos dados como sensíveis pode ser ilusória, na medida em que um conjunto de dados não sensíveis devidamente organizado e tratado pode conduzir a resultados mais intrusivos do que os primeiros".

A discriminação pode então surgir como resultado da aplicação das técnicas de tratamento de dados sensíveis, sendo este resultado considerado um efeito colateral perigoso, portanto, deve ser cuidado pelos Direitos Humanos, visto que ao se determinar quais indivíduos compõem um determinado perfil, pode-se gerar discriminação, por exemplo, pelo não acesso a determinadas informações, não oferta de determinado produto ou enquadramento de um grupo de pessoas a partir de rótulos pré-estabelecidos e que sejam contrários aos interesses de estados totalitários.

A questão do perfilamento ou *profiling* envolve diferentes aspectos técnicos e jurídicos, incluindo aspectos legislativos que devem levar em consideração as características intrínsecas dos sistemas computacionais frente a todas as possibilidades de tratamento de dados pessoais ou não, sendo mais preocupante a questão dos dados pessoais e dos dados sensíveis.

Deve-se ter em mente que a Internet possui vantagens, mas não se pode fechar os olhos para os problemas advindos da informação fragmentada a partir das bolhas informacionais e da discriminação advinda da caracterização de perfil (*profiling*). Estes problemas, muitas vezes passam despercebidos pelos usuários que veem o mundo sob uma configuração pré-estabelecida nos estados totalitários. A sociedade informacional é dinâmica, mas também é regida por quem detém a informação, a ponto de "a informação ser poder". Determinadas posições

em estados totalitários sobre o acesso à informação devem ser questionadas do ponto de visto dos anseios sociais dos indivíduos, visto não considerar a dinamicidade do mundo digital e não digital, de maneira não compatível com os princípios democráticos e, ao mesmo tempo sem permitir a tutela da esfera privada dos indivíduos que são usuários da rede mundial de computadores.

2.3 Mineração de dados e *Big Data*

As técnicas tradicionais de tratamento e exploração de dados deixaram de ser adequadas frente ao volume de dados coletados e armazenados, seja por uma empresa seja por um aplicativo ou serviço *on-line*, ou mesmo pelos governos. Pode-se aplicar técnicas mais sofisticadas que realmente possam "minerar" os dados e encontrar "tesouros" de informação e conhecimento.

A Mineração de Dados (*Data Mining*) tem como objetivo atender estas expectativas e pode ser definida por Fayyad, Piatetsky-Shapiro e Smyth (1996, p. 39-40) como "*nontrivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data*". De acordo com Castro e Ferrari (2016, p. 04), o termo Mineração de Dados foi cunhado uma vez que "explora uma base de dados (mina) usando algoritmos (ferramenta) adequados para obter conhecimento (minerais preciosos)". Continuam os autores explicando que (CASTRO e FERRARI, 2016, p. 04):

> Os dados são símbolos ou signos não estruturados, sem significado, como valores em uma tabela, e a informação está contida nas descrições, agregando significado e utilidade aos dados, como o valor da temperatura do ar. Por fim, o conhecimento é algo que permite uma tomada de decisão para a agregação de valor, então, por exemplo, saber, que vai chover no fim de semana pode influenciar sua decisão de viajar ou não para a praia.

Deste modo, entende-se que a Mineração de Dados compreende diversas tarefas, tais como: pré-processamento, extração e exploração de grandes quantidades de dados visando estabelecer padrões consistentes. Entende-se por padrões consistentes, por exemplo, o perfilamento (*profiling*) de usuários, o qual pode ser obtido por meio de regras de

associação ou, ainda, estabelecer quando um usuário utilizou um determinado aplicativo, sendo tal informação obtida por técnicas de sequenciamento temporal; para, então, por meio da Mineração de Dados, detectar-se relacionamentos sistemáticos entre variáveis (usuário e opção filosófica) ou determinar novos subconjuntos de dados (usuários potenciais que podem se ter uma determinada opção filosófica B sabendo-se que este usuário já se interessou pelo assunto A em uma determinada data e local). Todo este processo visa à obtenção de conhecimento.

Um exemplo da aplicação das técnicas de Mineração de Dados foi declarado na notícia[3] "O potencial do WhatsApp para o uso em mineração de dados: Mineração de dados é o processo de explorar grandes quantidades de dados à procura de padrões consistentes". Tal notícia explica que a Target, segunda maior rede varejista dos EUA, estava utilizando o processo de Mineração de Dados para entender os hábitos de compra de seus clientes e, ainda, que o Facebook "sabe quando você vai começar a namorar" cruzando dados sobre as interações dos usuários na rede social. Mostra ainda que existe um potencial enorme a ser explorado por técnicas que "vasculham" os dados de textos, tais como os utilizados no WhatsApp ou em VoIP[4]. Isto demonstra não somente o interesse nos dados dos usuários, mas o poder de processamento e tratamento de dados pessoais ou não derivados do uso dos serviços *online*.

Fayyad, Piatetsky-Shapiro e Smyth (1996, p. 38-39) apresentam diversas áreas que podem se beneficiar com a aplicação da Mineração de Dados, entre elas os autores citam: a) *marketing*: este setor se beneficia a partir de análises em bancos de dados de clientes para identificar

---

[3] Disponível em <http://tecnoblog.net/151635/potencial-whatsapp-mineracao-de-dados/> Acesso em 08 jun. 2016.

[4] De acordo com Bernal Filho (2017, p. 2) a "Comunicação de Voz em Redes IP, chamada de VoIP (*Voice on Internet Protocol*), consiste no uso das redes de dados que utilizam o conjunto de protocolos das redes IP para a transmissão de sinais de voz em tempo real na forma de pacotes de dados. A sua evolução natural levou ao aparecimento da Telefonia IP, que consiste no fornecimento de serviços de telefonia utilizando a rede IP para o estabelecimento de chamadas e comunicação de Voz." BERNAL FILHO, Huber. **Tutoriais Banda larga e VoIP**. 2017. Disponível em: <http://www.sj.ifsc.edu.br/~fabiosouza/Tecnico/Subsequente/Topicos%20em%20Telefonia/Tutorial%20Teleco%20VoIP.pdf>. Acesso em: 10 maio 2017.

diferentes grupos de clientes e prever seu comportamento, visando aumentar as vendas ou analisar o carrinho de compras e estabelecer relações, por exemplo: se o cliente comprou o produto X, também é provável que compre os produtos Y e Z; b) investimentos: nesta área a Mineração de Dados pode ser utilizada para gerenciar portfólios ou carteiras de ações; c) detecção de fraudes: podem ser monitoradas as fraudes de cartões de crédito estudando-se o padrão de comportamento do usuário de um determinado cartão ou, ainda, podem ser identificadas as transações financeiras que indicam atividade lavagem de dinheiro (*money-laundering activity*); d) manufatura: podem ser diagnosticados problemas de fabricação em aviões, por exemplo; telecomunicações: podem ser desenvolvidos sistemas que analisam episódios de fluxos de alarmes; e) limpeza de dados: é o processo de alteração ou remoção de dados em um banco de dados que está incorreto, incompleto, formatado incorretamente ou duplicado. A limpeza dos dados (*data cleansing* ou *data scrubbing*) pode ser realizada por meio de ferramentas que examinam sistematicamente os dados para detectar falhas usando regras, algoritmos e tabelas de consulta. A aplicação de ferramentas de limpeza de dados pode auxiliar um administrador de banco de dados a reduzir significativamente o tempo deste tipo de tarefa, caso a limpeza dos erros fosse realizada manualmente ou por processos simplificados; f) esportes: um sistema de mineração de dados pode auxiliar aos treinadores a organizarem e interpretarem dados dos jogos de um time ou seleção.

Fayyad, Piatetsky-Shapiro e Smyth (1996, p. 44) explicam que são dois os objetivos primários de alto nível da Mineração de Dados, a saber: previsão e descrição. A previsão envolve o uso de variáveis (atributos) ou campos no banco de dados para prever valores desconhecidos ou futuros de outras variáveis de interesse e a descrição se concentra em encontrar padrões interpretáveis por humanos descrevendo os dados. Os autores alertam que os limites entre a previsão e a descrição não são claros, visto que existem modelos híbridos, ou seja, modelos preditivos que também são descritivos.

Finalmente, aponta-se que a Mineração de Dados representa uma abordagem flexível para o gerenciamento de análises de documentos, estruturados (*web pages*) ou não (textos), visando estabelecer padrões consistentes. De uma maneira resumida pode-se concluir que a Mineração de dados é um processo iterativo e interativo

de descoberta de padrões e modelos novos (que não se tem ciência até o momento), válidos (genéricos no futuro), utilizáveis, abrangentes e compreensivos a partir de grandes volumes de dados (SON, 2017, p. 07).

Todo o tratamento de dados mencionado até o momento, somente é possível frente ao acúmulo de dados em proporções antes inimagináveis. O conceito que descreve este 'volume' de dados vem sendo conhecido como *Big Data*:

> Os dados das redes sociais online podem ser usados para extrair informações sobre padrões de interações interpessoais e opiniões. Esses dados podem auxiliar no entendimento de fenômenos, na previsão de um evento ou na tomada de decisões. Com a ampla adoção dessas redes, esses dados aumentaram em volume, variedade e precisam de processamento rápido, exigindo, por esse motivo, que novas abordagens no tratamento sejam empregadas. Aos dados que possuem tais características (volume, variedade e necessidade de velocidade em seu tratamento), chamamo-los de big data (FRANÇA *et al.*, 2014, p.8).

Pelo conceito apresentado, pode-se perceber que praticamente todo conteúdo produzido no âmbito da Internet, das redes sociais e dos aplicativos de *smartphones* e *tablets* pode ser considerado *Big Data*, o qual possui 3V's, de acordo com Kitchin (2014, p. 68), como características intrínsecas, a saber: volume, velocidade e variedade de tipos de dados estruturados ou não sendo frequentemente referenciados temporal e espacialmente, como já mencionaod neste capítulo.

Kitchin (2014, p. 67) pontua que a etimologia do termo *Big Data* foi estabelecida em meados da década de 90, sendo usado pela primeira vez por John Mashey para se referir a manipulação e análise de conjuntos volumosos de dados. O termo não despertou muito interesse no início, mas tornou-se um jargão utilizado constantemente na área de negócios e pela mídia.

Big Data tem sido considerado muito mais do que grandes quantidades de dados produzidos por *smartphones* e redes sociais. Manyika *et al.* (2011, p. vi) apontam que o Big Data alcança qualquer setor ou função da economia global: "*Big data - large pools of data that can be captured, communicated, aggregated, stored, and analyzed - is now part of every sector and function of the global economy.*". Os autores apresentam que: "*Each second of high-definition video, for*

example, generates more than 2,000 times as many bytes as required to store a single page of text. In a digitized world, consumers going about their day - communicating, browsing, buying, sharing, searching - create their own enormous trails of data." (MANYIKA *et al.*, 2011, p. 01). E, portanto, os autores definem *Big Data* de maneira subjetiva, mas ampla o suficiente para realmente englobar o que é *Big Data*: *"refers to datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze".* Não lá limitação de tamanho, tempo e lugar para *Big Data*. A visão dos autores é positiva no sentido de que existem evidências de que *Big Data* pode desempenhar um papel econômico significativo para o benefício, não somente do comércio privado, mas também das economias nacionais e seus cidadãos (MANYIKA *et al.*, 2011, p. 01). Pensamento contrário ao que pode ser encontrado nos estados totalitários.

Destaca-se que *Big Data* tem como cenário de fundo a sociedade transparente, visto que ao tornar os dados mais facilmente acessíveis aos interessados, em tempo hábil, mais especificamente em tempo real, pode-se agregar valor desde o setor público, reduzindo o tempo de busca e processamento de informações, até à indústria, a qual pode ver o prazo de fabricação diminuir e a qualidade aumentar (MANYIKA *et al.*, 2011, p. 05). Outra vantagem de *Big Data* é a real possibilidade de se aplicar análises sofisticadas que podem melhorar substancialmente a tomada de decisões, minimizar riscos e descobrir conhecimentos valiosos que, de outra forma, permaneceriam ocultos (MANYIKA *et al.*, 2011, p. 05).

Mas existem problemas como os já tratados neste artigo, a ponto de Manyika *et al.* (2011, p. 15) questionar: "*Is big data simply a sign of how intrusive society has become, or can big data, in fact, play a useful role in economic terms that can benefit all societal stakeholders?*", mencionando a sociedade intrusiva que surgiu com o alto grau de vigilância (*surveillance*) que não somente atinge cada indivíduo, mas tornou-se uma faceta da vida em um mundo conectado e globalizado (MARX, 2002). A vigilância tornou-se uma prática corriqueira frente à quantidade de câmeras digitais, seja em ambiente público ou privado, independentemente do indivíduo e lugar. Todos podem ser observados, mesmo aqueles que não estejam relacionados a atos ilícitos. O interesse pelos dados em tempo real vem caracterizando a prática de

escuta no meio digital (*eavesdropping*), ou seja, a interceptação em tempo real de comunicações privadas por meio de celulares, *smartphones*, mensagens eletrônicas e instantâneas, fax ou videoconferência. Esta prática deve ser diferenciada da conhecida escuta em uma linha telefônica convencional por métodos técnicos, a qual é denominada de escuta telefônica (*wiretapping*). (ROUSE e AUDIN, 2017).

Dados e mais dados. Esta é a realidade. Vive-se imerso em dados que são coletados, capturados, processados e analisados, mas o uso inadequado ou com interesses contrários aos Direitos Humanos podem comprometer a sociedade informacional que está estruturada não somente na informação como objeto, mas nos indivíduos que operam a dinâmica da informação.

3. O direito de acesso à informação como requisito para concretização da democracia

O direito de acesso à informação é relacionado à possibilidade de concretização do ideal democrático. A conexão é facilmente compreendida. A democracia, compreendida como um modelo de governo que permite a participação dos governados nas decisões, demanda a informação. A participação dos indivíduos é concretizada com sua manifestação (SALHANY, 1986) e só é possibilitada na medida em que conheçam os temas que serão debatidos e decididos, na medida em que tenham acesso aos diferentes argumentos e aos dados necessários para que possam refletir e formular sua própria opinião. Na essência do regime democrático está a possibilidade de participação e ela somente pode ser exercida na medida em que os indivíduos podem ser informados sobre os assuntos que digam respeito ao governo.

3.1 instrumentos internacionais de proteção ao direito informação

O direito a receber informação está intimamente conectado com a necessidade de transparência, exigida de governos em todo o globo. O artigo 19 da Declaração Universal de Direitos Humanos estabelece que

> Todo o homem tem direito a liberdade de pensamento, consciência e religia o; este direito inclui a liberdade de mudar de religia o ou crença e a liberdade de manifestar essa religia o ou crença, pelo ensino, pela pra tica, pelo culto e pela observâcia, isolada ou coletivamente, em pu blico ou em particular.

Em 2003, a adoção da Declaração de Princípios da Conferência de Cúpula da Sociedade de Informação expressa a relevância da democracia e da universalidade, indivisibilidade e interdependência de todos os direitos humanos e liberdades fundamentais. Neste sentido, reiterou a importância do direito de expressão, para a Sociedade de Informação:

> We reaffirm, as an essential foundation of the Information Society, and as outlined in Article 19 of the Universal Declaration of Human Rights, that everyone has the right to freedom of opinion and expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[5]

Em sentido próximo, a Declaração de Maputo, elaborada na Conferência da Unesco sobre Liberdade de expressão, Acesso à informação e Empoderamento das pessoas, realizada em 2008, apela aos Estados membros para

> To foster the free flow of information through policies founded on the four key principles of inclusive knowledge societies: freedom of expression, equal access to quality education, universal access to information, and respect for cultural diversity;…..
> … To prevent measures that hinder freedom of expression on Internet, particularly website censorship…[6]

---

[5] Nós reafirmamos, como um fundamento essencial da Sociedade de Informação, e como estabelecido no artigo 19 da Declaração Universal de Direitos Humanos, que todos têm o direito de opinião e expressão; que esse direito inclui a liberdade de ter opiniões sem interferências Tradução livre.

[6] Promover a livre circulação de informações através de políticas baseadas nos quatro princípios fundamentais das sociedades do conhecimento inclusivas: liberdade de expressão, igualdade de acesso à educação de qualidade, acesso universal à informação e

O direito de se expressar livremente está intimamente relacionado ao direito de informação, eis que a expressão é dependente do quanto o indivíduo tem acesso às informações e, ao mesmo tempo, o quanto de informações ele consegue fazer chegar a outros indivíduos. A informação não é objeto estático, é dinâmico e para se fortalecer e fortalecer os informados necessita ser veiculada. A tecnologia de informação e de comunicação (TIC) cria, desenvolve e distribui ferramentas *online* que permitem que os cidadãos aprofundem o exercício destes direitos. Ao mesmo tempo, diferentes governos têm desenvolvido métodos eficientes tanto para filtrar informações quanto para monitorar os usuários da internet, oferecendo, muitas vezes, ameaças aos direitos aqui mencionados.

A despeito da obrigação dos Estados de proteger direitos humanos, algumas situações reais demonstram que os governos atuam para violar o direito de informação. Por diversas vezes, contam com a cumplicidade de empresas da área de TIC para realizar restrições seja por meio de filtros ou de técnicas de Mineração de Dados aplicadas em *Big Data*, estruturando segmentação da informação, bem como a Internet fragmentada, tal qual apresentado anteriormente.

3.2 Violadores do direito: Estado e empresas

De fato, a história recente demonstra que o uso da tecnologia por governos autoritários reforça sua posição antidemocrática, impede que os cidadãos discutam assuntos que são de interesse público, restringe a capacidade de comunicação e evita que o regime seja contraposto.

A organização Repórteres sem Fronteiras divulga uma lista de Estados que censuram o fluxo de informações na internet, entre eles estão, Cuba, Irã, Myanmar/Burma, Coréia, Síria, Vietnam[7]. Todavia, é possível que o caso mais conhecido de interferência de um Estado sobre

respeito pela diversidade cultural ...Para evitar medidas que impeçam a liberdade de expressão na Internet, particularmente a censura de sítio eletrônico... Tradução livre.

[7] Disponível em https://rsf.org/en/rsf_search?key=internet%20censorship, acesso em 03.02.17.

as informações compartilhadas na internet seja o do Grande Firewall da China, termo utilizado para relacionar o mecanismo de segurança digital denominado de *firewall* à muralha da China. Deve-se ter em mente que mecanismos de segurança digital são elementos importantes do ponto de vista de segurança tanto da infraestrutura de rede quanto dos dados e informações, visto que são muitas as ameaças aos sistemas informatizados que podem possibilitar desde o uso indevido de informações sigilosas quanto à paralisação ou negação de serviços *online*, sem deixar de lado os crimes e fraudes de informática que podem ser realizados no ambiente digital.

Assim, *firewall*, tecnicamente, pode ser entendido como "sistemas de segurança com hardware e/ou software especializados para impedir que estranhos invadam as redes privadas"[8], por exemplo de uma empresa, instituição ou órgão governamental. Estes mecanismos podem ser implantados também na Internet, de modo a interceptar pacotes de dados que circulam na rede, visando examinar suas características e rejeitar arquivos ou mensagens ou tentativas de acesso não autorizadas. Isto é importante quando se pretende proteger uma rede privada das diferentes categorias de *malware* existentes no ambiente digital. Vale esclarecer que *malware* (*malicious software* ou software malicioso) é espécie em que se enquadram qualquer categoria de programa mal-intencionado, podendo-se citar: cavalo de Tróia, vírus, *adware*, *hijacker*, entre outros.[9] Deve-se esclarecer que nem todos os códigos maliciosos são vírus.

Porém, a aplicação de *firewall* pode ser modificada para verificar e filtrar todo o fluxo de dados, violando não somente a integridade dos dados, mas também a confidencialidade dos dados. Na China, os aspectos de censura e vigilância são relevantes:

> China's system of Internet censorship and surveillance is the most advanced in the world. While tens of thousands of people are employed by the Chinese government and security organs to implement a system of political censorship, this system is also aided by extensive corporate and private sector cooperation—including by some of the world's major international technology and Internet companies. In China, the active

[8] LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação**, p. 176.

[9] LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação**, p. 262.

> role of censor has been extended from government offices into private companies. Some companies not only respond to instructions and pressures from Chinese authorities to censor their materials, they actively engage in self-censorship by using their technology to predict and then censor the material they believe the Chinese government wants them to censor.[10]

Há diferentes meios para que uma empresa da área de Tecnologia de Informação e Comunicação (TIC) possa auxiliar governos a violar os direitos de expressão e informação. A postura das empresas as revela como cúmplices de censura, em clara violação aos instrumentos internacionais sobre o tema, por meio de colaboração deliberada com o governo. Em 2005, a Microsoft[11] foi alvo de críticas por ter censurado palavras como 'democracia' e 'liberdade' em títulos de blogs chineses, a pedido do governo. Em 2006, o Google lançou sua ferramenta de censura, denominada Google.cn, que informa o usuário quando o resultado de sua busca foi censurado e não provê os chineses de serviços como email ou blogs, para evitar o recebimento de demandas, do governo, para a entrega de dados dos usuários. A ferramenta Skype censura determinadas palavras em mensagens de texto e o faz para cumprir a legislação local, a empresa, no entanto, não informa aos usuários que pratica a censura e muito menos, qual exatamente é a política adotada.

Sem dúvida, no entanto, o caso mais conhecido de violação de direitos humanos relacionado à empresas da área de TIC, na China, é o

---

[10] Human Rights Watch. Race to the bottom, Summary, Disponível em https://www.hrw.org/reports/2006/china0806/, acesso em 07.06.17. O sistema chinês de censura e vigilância da Internet é o mais avançado do mundo. Enquanto dezenas de milhares de pessoas são empregadas pelo governo chinês e pelos órgãos de segurança para implementar um sistema de censura política, esse sistema também é auxiliado por uma ampla cooperação entre empresas e setor privado - incluindo algumas das principais empresas internacionais de tecnologia e internet do mundo. Na China, o papel ativo da censura foi estendido de escritórios governamentais para empresas privadas. Algumas empresas não só respondem às instruções e pressões das autoridades chinesas para censurar seus materiais, elas se envolvem ativamente na autocensura usando sua tecnologia para prever e então censurar o material que eles acreditam que o governo chinês quer que eles censurem. Tradução livre.

[11] Todos os casos aqui mencionados estão no relatório denominado Race to the Bottom da Human Rights Watch, Disponível em https://www.hrw.org/reports/2006/china0806/, acesso em 07.06.17.

do Yahoo!. A empresa entregou ao governo informações sobre um repórter e editor do jornal denominado Contemporary Business News. Shi Tao foi levado de sua residência, em 2004, preso sob acusações secretas advindas da publicação de detalhes contidos em um memorando secreto do governo intitulado "Informativo sobre o Atual Trabalho de Estabilização". No caso perante a Corte, foi alegado que ele tomou notas sobre o memorando enquanto ele estava sendo discutido em um encontro editorial do jornal e algumas horas depois, enviou uma minuta de seu conteúdo, por email, para o exterior, para ser publicado em um fórum na rede, sob um pseudônimo. As provas foram colhidas com o auxílio da Yahoo! Holdings Ltd., situada em Hong Kong, que fez a conexão do endereço de IP utilizado para enviar o email da conta de email que Shi Tao mantinha no Yahoo com um computador localizado na sede do jornal. O conteúdo do memorando dava conta de atividades de ativistas pela democracia no 15o. aniversário da repressão no Protesto de Tiananmen, assim como a ameaça representada por Falun Gong[12] e o aumento no número de incidentes, assim como o perigo da existência de determinados conteúdos na internet. O memorando ainda alertava os profissionais da mídia a não manifestar quaisquer opiniões sobre as políticas do governo e a reportar contatos suspeitos entre ativistas pela democracia e jornalistas. Shi Tao foi condenado, por divulgar segredos de Estado no exterior, a dez anos de prisão e após, dois anos de privação de seus direitos políticos[13].

Segundo o Relatório Race to the Bottom da Human Rights Watch[14], os instrumento de censura da Yahoo! são tão severos quanto os utilizados pelas empresas chinesas de internet e, assim, muito mais rigorosos dos que aqueles utilizados pelo Google, por exemplo.

Tratam-se, no geral, de empresas que têm sido cúmplices do Governo Chinês na censura de informação política ou religiosa,

---

[12] Trata-se de uma prática de auto-cultivo da Escola Buda. O governo chinês se sente ameaçado pela prática por ela reunir muitos adeptos. O governo ainda alega que vários dos manifestantes da Praça de Tiananmen eram adeptos da prática. Para saber mais http://pt.falundafa.org/inicio.html

[13] Os fatos do caso e as decisões estão disponíveis em Law Professors Blog Network, em http://lawprofessors.typepad.com/china_law_prof_blog/files/ShiTao_verdict.pdf, acesso em 10.07.17.

[14] Disponível em https://www.hrw.org/reports/2006/china0806/, acesso em 07.06.17.

aceitando demandas do governo sem apresentar qualquer obstáculo. Este tipo de censura decorre da caracterização de perfil (*profiling*) que resulta da aplicação das técnicas de Mineração de Dados sobre *Big Data*, como explicado anteriormente neste artigo. Deve-se esclarecer que o *firewall* é o primeiro nível de verificação e filtragem do fluxo de dados, de modo a direcionar o fluxo de dados à formação de *Big Data* para posterior aplicação das técnicas de Mineração de Dados obtendo-se tanto a caracterização de perfil quanto a segmentação dos dados de acordo com os interesses estabelecidos, que podem ser políticos, religiosos, comerciais, industriais e até mesmo de censura e/ou vigilância.

É necessário que se diga, no entanto, que o governo chinês utiliza-se deste recurso de acordo com a legislação daquele país. De fato, há mais de sessenta regulamentações diferentes sobre o uso da internet, aplicáveis à diferentes atores como empresas, governos províncias e organizações. A alegação das empresas, em suas defesas, é que não teriam acesso ao mercado chinês se não cumprissem com as regras impostas pela legislação doméstica. Esse é um desafio real para empresas que buscam novos mercados para seu desenvolvimento e devem enfrentar percalços de ordem internacional, como os instrumentos internacionais de proteção aos direitos humanos, para atuar.

Diante dos *standards* internacionais que impõe que os Estados protejam direitos humanos e dos princípios que se aplicam à atuação de empresas, há, à evidência, um conflito entre a postura das empresas em relação às suas responsabilidades e as demandas de determinados Estados. Os Estados são os sujeitos primários de Direito Internacional[15] por isso, são os atores que firmam tratados internacionais, de acordo com o que prevê a Convenção de Viena sobre o Direito dos Tratados, de 1969. Da dicção da Carta das Nações Unidas, do Pacto Internacional sobre os Direitos Civis e Políticos (1966) e do Pacto Internacional sobre os Direitos Econômicos e Sociais (1966) conclui-se que são os Estados obrigados a promover o respeito universal aos direitos humanos. Todavia, estes são instrumentos forjados no pós Segunda Guerra, quando não se podia fugir à conclusão de que os Estados podiam ser os responsáveis por enormes violações de direitos. Do pós-Segunda Guerra para hoje, muito aconteceu, várias outras violações de direitos foram

[15] REZEK, Francisco. Direito Internacional Público, p.181.

catalogadas e a conclusão inevitável é que o Estado deixou de ser o único violador de direitos humanos.

Neste sentido, hoje, as empresas são reconhecidas como importantes atores neste cenário. O crescimento econômico que apresentam e sua capacidade de operar em vários Estados, trazem diferentes desafios para o efetivo respeito aos direitos humanos. Assim, a comunidade internacional, atenta ao fato, passou a se indagar sobre os compromissos que poderiam ser exigidos das empresas diante da relação de suas atividades e seu potencial para violar direitos humanos, assim como sobre as possibilidades de responsabilização das mesmas por tais violações. As primeiras iniciativas datam da década de 70 do século passado, mas é somente nos anos 2000 que o então Secretário-Geral da ONU, Kofi Annan, dá um passo importante para a evolução do tema. Em 2005, nomeia como seu Representante Especial para Empresas e Direitos Humanos o professor de Harvard, John Ruggie, com mandato para "elaborar padrões de responsabilidade das empresas transnacionais e dos Estados na garantia de que os direitos humanos fossem observados. Assim surgem os denominados Princípios das Nações Unidas para Empresas e Direitos Humanos, aprovados pelo Conselho de Direitos Humanos em 2011"[16].

4. Possibilidades de responsabilização

Apesar da evolução da discussão no âmbito das Nações Unidas, não há, na atualidade, possibilidade de responsabilização de empresas perante Cortes internacionais de direitos humanos. O Estado continua sendo o protagonizador de violações e o único responsável.

A responsabilização, no entanto, pode e deve se dar nas jurisdições domésticas, em primeiro lugar, no local onde ocorrem e, se impossível, no domicílio da corporação. As possibilidades de responsabilização de empresas que violam direitos humanos por meio de atividades atribuíveis à subsidiárias também é bastante debatida, eis que, invariavelmente, há disputas judiciais sobre a possibilidade de alcançar a empresa-matriz ou a possibilidade de estrangeiros litigarem

[16] SILVA, Ana Rachel; PAMPLONA, Danielle Anne. Os princípios orientadores das Nações Unidas para empresas e direitos humanos: houve avanços? p. 153.

buscando responsabilizar empresas sediadas fora de seu país de origem, e, se isso não ocorre, há ainda a dificuldade imposta pelas estruturas disponíveis nos ambientes domésticos aos quais caberia a decisão sobre a responsabilidade da empresa.

Isso significa dizer que a responsabilização deste setor resta nas mãos das jurisdições nacionais que decidem os pedidos elaborados por aqueles que tiveram seus direitos violados. Qualquer outra movimentação serve, tão somente, para fomentar a discussão e a conscientização das empresas do setor. Neste sentido é que a União Europeia elaborou um guia[17] para implementação dos Princípios Ruggie por empresas do setor TIC, pavimentando a estrada para sua incorporação pelo setor. O guia esclarece que todos os direitos humanos internacionalmente reconhecidos são protegidos pelos Princípios Ruggie mas estabelece quais são os direitos que têm maior potencial de serem violados por este setor. A ausência de um Estado capaz de garantir adequadamente os direitos humanos de seus cidadãos não altera a responsabilidade das empresas do setor em respeitar os mesmos direitos, mas torna sua atuação mais complexa. O modo com que os Estados atuam tem grande influência para este setor, em especial quando o Estado demanda a corrupção de instrumentos tecnológicos aproveitando-se da demora da criação de regulamentação adequada – eis que o desenvolvimento tecnológico é mais rápido do que o legislativo; ou quando as leis que protegem as relações de trabalho são fracas ou sua aplicação não é fiscalizada adequadamente pelo Estado. Fomentar a aplicação dos Princípios forjados por Ruggie é um primeiro passo para aprofundar o respeito aos direitos humanos, todavia, a possibilidade de que um grande incremento na proteção possa ocorrer sem um instrumento vinculante ou legislação doméstica rigorosa e aplicada com precisão, é bastante pequena.

---

17 European Commission. ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, p.7 e ss. Disponível em http://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf, Acesso em 30.07.2017.

5. Considerações finais

Sobram situações fáticas que indicam a importante participação das empresas do setor de TIC para a ocorrência de violações de direitos humanos. No geral, as possibilidades de violação derivam de legislações inexistentes ou de instituições fracas. No desenvolvimento das atividades do setor analisado no presente texto, vários são os casos em que há cumplicidade da corporação com o Estado em que ela está desenvolvendo suas atividades.

Por meio das atividades de mineração de dados e de *profiling*, as empresas de TIC podem arregimentar dados e dividi-los com Estados inclinados ao autoritarismo. Ainda que haja um esforço da comunidade internacional para responder a estas violações, os instrumentos voluntários até então criados não são capazes de surtir o efeito desejado, nem na prevenção das ocorrências, nem nas reparações necessárias.

Referências

BOURDIEU, Pierre. **O campo científico**. In: ORTIZ, Renato (Org.) Pierre Bourdieu. Sociologia. São Paulo: Editora Ática, 1994.

CASTRO, Leandro Nunes de; FERRARI, Daniel Gomes. **Introdução à mineração de dados**. Conceitos básicos, algoritmos e aplicações. São Paulo: Saraiva, 2016.

DRAKE, William J.; CERF, Vinton G.; KLEINWÄCHTER, Wolfgang. **Internet Fragmentation**: An Overview. World Ecomonic Forum, Committed to Improving the State of the World, 2016.

DUHIGG, Charles. **The Power of Habit**: why we do what we do, and how to change. 1st. ed. Random House. 2012.

EUROPEAN COMMISSION. **ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights**. Disponível em http://ec.europa.eu/antitrafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf, Acesso em 30.07.2017.

FAYYAD, Usama; PIATETSKY-SHAPIRO, Gregory; SMYTH, Padhraic. **From data mining to knowledge discovery**: an overview. *AI Magazine*, American Association for Artificial Intelligence, Vol. 17, No 3, 1996. p. 37-54. Disponível em:

< https://www.aaai.org/ojs/index.php/aimagazine/article/viewFile/1230/1131 > . Acesso em: 20 jul. 2017.

FERRARIS, Valeria; BOSCO, Francesca; CAFIERO, G.; D'ANGELO, Elena; SULOYEVA, Y., **Working paper: defining profiling**. United Nations Interregional Crime and Justice Research Institute (UNICRI), December, 2013. Disponível em: <www.unicri.it/news/files/Profiling_final_report_2014.pdf>. Acesso em: 20 jul. 2017.

FRANÇA, Tiago Cruz; FARIA, Fabrício Firmino de; RANGEL, Fabio Medeiros; FARIAS, Claudio Miceli; OLIVEIRA, Jonice. **Big Social Data: Princípios sobre coleta, tratamento e análise de dados sociais**. Artigo publicado nos anais do XXIX Simpósio Brasileiro de Banco de Dados (SBBD) 2014. Curitiba. 2014, p. 8. Disponível em: <http://www.inf.ufpr.br/sbbdsbsc2014/sbbd/proceedings/artigos/pdfs/127.pdf >. Acesso em: 20 jul. 2017.

HILDEBRANDT, Mireille. Who is Profiling Who? Invisible Visibility. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) **Reinventing Data Protection?**. Springer, Dordrecht, 2009. p.239-252. Disponível em: <https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_14>. Acesso em: 20 jul. 2017.

HUMAN RIGHTS WATCH. **Race to the Bottom.** Disponível em https://www.hrw.org/reports/2006/china0806/, acesso em 07.06.17.

KITCHIN, Rob. **The data revolution**: big data, open data, data infrastructures & their consequences. Los Angeles: SAGE Publications Ltd., 2016.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação**. Rio de Janeiro: Livros Técnicos e Científicos S.A., 1999.

LAW PROFESSORS BLOG NETWORK, **Caso Shi Tao**. Disponível em http://lawprofessors.typepad.com/china_law_prof_blog/files/ShiTao_verdict.pdf, acesso em 10.07.17.

MACEDO, Daniele. **Confira oito sites populares que são proibidos na China**: a censura chinesa controla com mãos de ferro o acesso da população à internet. Quando não são banidos, sites têm parte do conteúdo bloqueado. Veja.com, 2016. Disponível em: <http://veja.abril.com.br/tecnologia/confira-oito-sites-populares-que-sao-proibidos-na-china/>. Acesso em: 20 jul. 2017.

MANYIKA, James et al.. **Big data**: The next frontier for innovation, competition, and productivity. McKinsey Global Institute, 2011.

MARX, Gary T. What's new about the "new surveillance"? Classifying for Change and Continuity. **Surveillance & Society**, Vol. 1. No. 1. 2002. p. 9-29.

ONU Organização das Nações Unidas. **Declaração Universal dos Direitos Humanos.** Disponível em: <http://www.onu.org.br/img/2014/09/DUDH.pdf>. Acesso em: 15.jul.17.

PARISER, Eli. **O Filtro Invisível**: o que a internet está escondendo de você. Trad. Diego Alfaro. Rio de Janeiro: Zahar, 2012.

PINHEIRO, Alexandre de Sousa. **Privacy e protecção de dados pessoais**: a construção dogmática do direito à identidade informacional. Lisboa: AAFDL, 2015.

REPORTERES SEM FRONTEIRAS. **World press freedom index**. Disponível em https://rsf.org/en/rsf_search?key=internet%20censorship, acesso em 03.02.17.

REZEK, Francisco. *Direito Internacional Público: Curso Elementar.* 11. ed. rev. atual. São Paulo: Saraiva, 2005.

ROUSE, Margaret; AUDIN, Gary. **Definition of eavesdropping**. Tech Target, 2017. Disponível em: <http://searchfinancialsecurity.techtarget.com/definition/eavesdropping>. Acesso em: 20 jul. 2017.

SALHANY, Roger. **The origin of rights**. Michigan: Carswell, 1986.

SCHWAB, Klaus. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SILVA, Ana Rachel; PAMPLONA, Danielle Anne. Os princípios orientadores das Nações Unidas para empresas e direitos humanos: houve avanços? In BENACCHIO, Marcelo (Coord.), A sustentabilidade das relações entre empresas transnacionais e direitos humanos. Curitiba: CRV, 2016, pp. 147-168.

SON, Nguyen Hung. **Introduction to KDD and data mining**. University of Warsaw, Faculty of Mathematics, Informatics and Mechanics, 2017. Disponível em: <https://www.mimuw.edu.pl/~son/datamining/DM/1-intro.pdf>. Acesso em: 20 jul. 2017.

MUTAÇÕES DA PRIVACIDADE E A PROTEÇÃO DOS DADOS PESSOAIS

Têmis Limberger[1]

1 INTRODUÇÃO

Na sociedade moderna as pessoas se exibem constantemente nas redes sociais, conectadas à internet, nestas situações, são divulgadas imagens, disponibilizadas informações e opiniões sobre assuntos diversos e dados pessoais são facilmente fornecidos. A informação em rede potencializa a divulgação da comunicação, já que pode ser difundida rapidamente por todos os continentes e também, armazenada por um tempo indefinido, que pode ser perpétuo, considerando-se os recursos informáticos existentes.

Por isso, na época do advento da comunicação de massa, denominou-se a sociedade do espetáculo[2] e, posteriormente, a civilização do espetáculo[3]. Hodiernamente, na tentativa de democratização universal da cultura houve um empobrecimento da mesma, pois se tornou superficial. A cultura foi transformada em artigo de consumo de massa, aonde o espetáculo é a diversão.

Diante deste quadro, o direito à privacidade, que foi concebido inicialmente como o direito a estar só, não é mais reivindicado pela maioria da população contemporânea. Neste contexto, pergunta-se: acabou-se o direito à privacidade (morte da privacidade) ou ocorreu uma mutação da privacidade?

---

[1] Professora do Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos – UNISINOS. Pós-doutora em Direito pela Universidade de Sevilha, doutora em Direito Público pela Universidade Pompeu Fabra - UPF de Barcelona. Avaliadora "ad hoc" da Revista de Direito do Consumidor, da Revista Brasileira de Direitos Fundamentais e Justiça, da Revista Quaestio Iuris e da Revista Direito Público. Procuradora de Justiça do Ministério Público do Estado do Rio Grande do Sul. Membro do Instituto Brasileiro de Direito Eletrônico - IBDE, da Federación Iberoamericana de Asociaciones de Derecho e Informática - FIADI e da Rede Brasileira de Pesquisadores em Direito Internacional. Orientadora de Mestrado e Doutorado.

[2] DEBORD, Guy. *A sociedade do espetáculo*. Rio de Janeiro: Contraponto, 1997.

[3] LLOSA, Mario Vargas. *A civilização do espetáculo: uma radiografia do nosso tempo e da nossa cultura*. Rio de Janeiro:Objetiva, 2013.

Pretende-se responder à seguinte questão: como compatibilizar as informações públicas em rede e a proteção da privacidade, protegendo-se os dados pessoais dos que navegam na rede?

2 A DIVULGAÇÃO DA INFORMAÇÃO PÚBLICA E OS LIMITES JURÍDICOS

A ideia de uma esfera reservada, que não se fizesse pública é algo recente na história dos direitos humanos. Os antigos não tinham a noção de público e privado[4]. A distinção entre esfera pública e privada era desconhecida e haveria sido incompreendida para o *polítes*. Hannah Arendt[5] chegou a afirmar que: a vontade livre é uma faculdade virtualmente ignorada na antiguidade clássica. Na Grécia e em Roma, a liberdade era exclusivamente um conceito político. A conceituação público e privado é uma noção que se desenvolve, a partir Estado liberal.

O direito à privacidade, *The right to privacy*, surgiu nos Estados Unidos em 1890 por criação doutrinária de Samuel Warren e Louis Brandeis, publicada na *Harward Law Review*, em 1890[6]. O direito a ser deixado em paz, da expressão inglesa *the right to be let alone*, surge com a difusão generalizada da imprensa e sua possibilidade de interferir na vida privada. O direito norte-americano tutela o direito à privacidade, de forma ampla, sem distingui-la da intimidade.

A privacidade surge como uma criação do Estado Liberal. O proclamado direito a estar só[7]. Como direito de faceta liberal, o aspecto negativo é evidente. O cidadão se contentava com que o Estado não inteferisse na sua esfera de liberdade. Uma reação compreensível em contraposição ao Absolutismo Monárquico, até então vigorante. O Estado social apresenta a dimensão positiva dos direitos. O direito à privacidade não ficou ileso. Passará a ter uma faceta positiva, que se

---

4 SARTORI, Giovanni. *Teoría de la democracia*. Vol. 2. Madrid: Alianza Editorial, 1988, p. 352.

5 ARENDT, Hannah. *Entre o passado e o futuro*. 6ª ed. São Paulo: Perspectiva, 2009 (Debates; 64/ dirigida por Guinsburg). Que é a liberdade, p. 188/220.

6 WARREN, Samuel D.; BRANDEIS, Louis D. *The right to privacy*. Harvard Law Review, vol. IV, nº 5, p. 193-220, Dec., 1890.

7 LIMBERGER, Têmis. *O Direito à intimidade na era da informática: o desafio da proteção dos dados pessoais*. Porto Alegre: Livraria do Advogado, 2007, p. 55. Vide também PROSSER, Willian. *Privacy*. Califórnia Law Review, v. 48, n. 3, 1960, p. 389.

demonstrará, a partir do direito de acesso, retificação e cancelamento dos dados. O direito espanhol denomina *derecho al olvido* e os italianos como um espectro ao *diritto a la riservartezza*. Tal perspectiva é muito importante, pois as informações serão armazenadas por longo tempo. Assim, é essencial que o cidadão possa ter acesso ao conteúdo armazenado, modificá-lo e até mesmo cancelá-lo – direito ao esquecimento[8].

Frente ao fenômeno informático, desenvolveu-se a noção de autodeterminação informativa[9], que equivale à liberdade informática com um valor indiscutível na sociedade da informação[10]. Sua função consiste em garantir aos cidadãos direitos de informação, acesso e controle dos dados que lhes concernem. Essa faculdade não é intrassubjetiva, mas sim uma autodeterminação do sujeito no seio de suas relações com os demais cidadãos e o poder público. O livre desenvolvimento da personalidade estaria dividido em duas liberdades. De um lado, a liberdade para decidir realizar ou não determinados atos e a faculdade para comportar-se ou atuar de acordo com essa decisão. De outro, a autodeterminação informativa referente à liberdade do indivíduo para determinar se deseja tornar públicas informações a seu

---

8 MARTINS, Guilherme Magalhães. O direito ao esquecimento na Internet. In: MARTINS, Guilherme Magalhães (Coord.). *Direito privado e internet*. São Paulo: Atlas, 2014. p. 3/28.

9 PÉREZ LUÑO, Antonio Enrique. *Manual de informática y derecho*. Barcelona: Editorial Ariel S.A., 1996, p. 44.

10 Sustentando a mesma posição da tese afirmativa de um direito, a partir do artigo 18.4 da CE: DAVARA RODRIGUEZ, Miguel Ángel. *Manual de Derecho Informático*. Madrid: Aranzadi, 1993, p. 65. MURILLO, Pablo Lucas. *El derecho a la autodeterminación informativa*. Madrid: Tecnos, 1990, p. 157-8 (Temas Clave de la Constitución Española) e Informática y protección de datos personales. Cuadernos e Debates, Madrid nº 43, 1993, p. 47-87. HIGUERAS, Manuel Heredero. *La nueva ley alemana de protección de datos*. Boletín de Información del Ministerio de la Justicia, ano XLVI, nº 1630, 1992, p. 1765. RUIZ MIGUEL, Carlos. *La configuración constitucional del derecho a la intimidad*. Madrid: Tecnos, 1995, p. 94/7. BENDA, Ernesto. *Dignidad Humana y derechos de la personalidad*. In: Manual de Derecho Constitucional. Madrid: Marcial Pons, 1996, p. 132. Em sentido contrário, não reconhecendo o nascimento de um novo direito fundamental: DENNINGER, E.. *El derecho a la autodeterminación informativa*. In problemas actuales de la documentación y la informática jurídica, PÉREZ LUÑO, Antonio E. (Org.). Madrid: Tecnos, 1987, p. 271. Vide também LIMBERGER, Têmis. *O Direito à intimidade na era da informática: o desafio da proteção dos dados pessoais*. Porto Alegre: Livraria do Advogado, 2007, p. 63/102.

respeito, bem como a quem cedê-las e em que ocasião. Na época, foi paradigmática a sentença do Tribunal Constitucional Federal Alemão com relação à Lei do Censo[11], em 1983.

Com a expansão das novas tecnologias em rede, em 27/2/2008, o Tribunal Constitucional Federal Alemão atualizou a autodeterminação informativa, a partir do novo direito fundamental à garantia de confidencialidade e integridade dos sistemas técnico-informacionais[12], acentuando a aludida migração das relações sociais e condução da vida do indivíduo para o ambiente técnico-informacional. A decisão ficou restrita à atuação do poder público, mas é amplamente reconhecido o impacto que pode causar no setor privado, igualmente.

A Diretiva Comunitária 95/46, foi o primeiro marco regulatório que aglutinou as disposições principais para assegurar a proteção dos dados pessoais e a livre circulação de dados aos países comunitários. Muitos Estados, na época, tiveram que adequar suas legislações internas, para compatibilizá-las com a regra comunitária unificada.

A discussão teórica a respeito de ser a autodeterminação informativa um novo direito ou faceta do direito à intimidade evoluiu para a positivação do reconhecimento da proteção dos dados pessoais, de forma autônoma. Isto significa, a proteção de todos os dados de caráter pessoal que digam respeito ao cidadão. Esses dados devem ser objeto de um tratamento legal, com finalidade específica e com consentimento da pessoa interessada.

Hodiernamente, na Comunidade Europeia, a proteção dos dados pessoais é um direito autônomo com relação à intimidade ou

---

11 Sentença de 15/12/1983, do Tribunal Constitucional Alemão, *Boletín de Jurisprudencial Constitucional*, nº 33, janeiro 1984, p. 137. A questão discutida, neste julgamento, que se tornou paradigmático, era com relação à Lei do Censo, que fazia demasiadas perguntas, o que poderia atentar diretamente contra os direitos fundamentais de liberdade de opinião, inviolabilidade de domicílio e liberdade de expressão. O objetivo do Tribunal era aprofundar as bases constitucionais da proteção de dados relativas à pessoa. A norma básica em referência era o direito geral de respeito à personalidade garantido pelo art. 2.1 (Direito Geral de Personalidade), combinado com o art.1.1 (a dignidade da pessoa humana) da Lei Fundamental de Bonn.

12MENKE, Fabiano. *A proteção de dados e o novo direito fundamental à garantia de confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão* "in" Direito, Inovação e Tecnologia, vol. I. Coordenadores: Gilmar F. Mendes, Ingo W. Sarlet e Alexandre Z. Coelho, São Paulo: Saraiva, 2015, pp. 205/230.

privacidade, nos países europeus, veja-se o Tratado de Lisboa, artigo 16-B[13], que ratificou a Carta de Nice[14], contemplando o direito fundamental à proteção dos dados pessoais (artigo 8º), em caráter autônomo à intimidade (artigo 7º). O diploma explicitador dos direitos fundamentais da União Europeia demonstra estar sintonizada com as questões oriundas do ciberespaço.

A atual proposta de Regulamento do Parlamento Europeo e do Conselho (regulamento geral sobre a proteção de dados)[15], estabelece dentre os direitos do titular dos dados, a retificação e o cancelamento. O artigo 17 confere ao titular dos dados o direito a ser esquecido[16]. Desenvolve e especifica mais detalhadamente o direito de cancelamento já consagrado no artigo 12º alínea "b" da DC 95/46/CE, e prevê as

---

13 UNIÃO EUROPEIA. *Jornal Oficial da União Europeia*. Tratado de Lisboa. C 306, 50º ano, 17 de dezembro de 2007. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:FULL:PT:PDF>. Acesso em: 25 mar. 2016.

14 UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia*, de 07 de dezembro de 2000. Carta de Nice. Disponível em: <http://www.europarl.europa.eu/charter/default_pt.htm>. Acesso em: 25 mar. 2016.

15 Comissão Europeia analisa Proposta de Regulamento do Parlamento Europeu e do Conselho de Bruxelas, de 25/11/2012. Nesse sentido, vide novidades referidas por SÁNCHEZ BRAVO, Álvaro A. *Hacia un nuevo marco europeo de protección de datos personales: empoderamiento de los ciudadanos en la sociedad tecnológica*. In: Sociocibernética e Infoética: contribuición a una nueva cultura y praxis jurídica. (Org.) Yarina Amoroso Fernández. 1ed. Habana - Cuba: Editorial UNIJURIS, 2015, v. 1, p. 123, no que diz com a Transparencia, como *toda información dirigida al público, debe ser fácilmente acesible y fácil de entender utilizándose un lenguage sencillo y claro. (…) El derecho al olvido, además, del clásico derecho a la "retificación de los datos"*. Existe projeto para atualizar as disposições comunitárias. Em palestra proferida na Universidade de Nova York, o executivo da *Google* Eric Schmidt afirmou que a *internet* precisa de um botão de *delete,(...)* A falta de um botão *delete* na *internet* é um problema significativo. (*Google's Schmidt:The internet needs a delete Button.* Google's Executive Chairman Eric *Schmidt says mistakes people make when young can haut them forever.* Disponível em: <http://news.cnet.com/8301-1023_3-57583022-93/googles-schmidt-the-internet-needs-a-delete-button/>. Acesso: em 10 mai. 2013.

16 A vice-Presidente da Comissão de Justiça da União Europeia, Viviane Reding, apresentou proposta de revisão das diretivas anteriores, para que se contemple, expressamente, o direito ao esquecimento dos usuários de *internet*, afirmando que "*al modernizar la legislación, quiero clarificar especificamente que las personas deben tener el derecho, y no solo la posibilidad, de retirar su consentimiento al procesamiento de datos* [...]" e que o primeiro pilar da reforma será *el derecho a ser olvidado:"un conjunto completo de reglas nuevas y existentes para afrontar mejor los riesgos para la privacidad en Internet"* Disponível em: <http://www.20minutos.es/noticia/991340/0/derecho/olvido/facebook/>. Acesso em 2 mai. 2013.

condições do direito a ser esquecido, incluindo a obrigação do responsável pelo tratamento que tornou público os dados pessoais de informar os terceiros sobre o pedido em causa de cancelamento de quaisquer ligações para esses dados ou cópias ou reproduções que tenham sido efetuadas.

Dentre os princípios que já eram elencados, anteriormente, são agregados outros, dentre os quais o Princípio da Transparência. O artigo 11 introduz a obrigação de os responsáveis pelo tratamento fornecerem informações transparentes, de fácil acesso e compreensão, que se inspira especialmente na Resolução de Madrid sobre as normas internacionais em matéria de proteção de dados pessoais e da vida privada[17].

No Brasil, os direitos à intimidade e à privacidade estão referidos no artigo 5º, X, da Constituição Federal - CF, reconhecendo a distinção proveniente da doutrina e jurisprudência alemãs, da teoria das esferas ou dos *círculos concêntricos*[18]. As esferas da vida privada comportam o grau de interferência que o indivíduo suporta com relação a terceiros. Para tal, leva-se em consideração o grau de reserva do menor para o maior. Assim, no círculo exterior está a privacidade; no intermediário, a intimidade; e, no interior desta, o sigilo. Deste modo, a proteção legal torna-se mais intensa, à medida que se adentra no interior da última esfera.

A proteção dos dados pessoais não é direito positivado em muitos países latino-americanos[19], porém se deve conferir-lhe alguma tutela. Se não é possível como direito autônomo, pode-se proteger como consequência do direito à intimidade. No Brasil, o Marco Civil da Internet (Lei nº 12.965/2014) prevê a proteção dos dados pessoais (art. 3º, III) na forma da lei, sem que até o momento exista disposição legislativa para regular a matéria. A necessidade de proteção à privacidade, também é estatuída pelo Marco Civil da Internet (art. 3º, II e art. 8).

---

[17] SÁNCHEZ BRAVO, Álvaro A. *Hacia un nuevo marco europeo de protección de datos personales: empoderamiento de los ciudadanos en la sociedad tecnológica*. In: Sociocibernética e Infoética: contribuición a una nueva cultura y praxis jurídica. (Org.) Yarina Amoroso Fernández. 1ed. Habana - Cuba: Editorial UNIJURIS, 2015, v. 1, p. 124.

[18] COSTA JR., Paulo José da. *O direito a estar só: tutela penal da intimidade*. São Paulo: RT, 1970, p. 31, citando HENKEL, Der Strafschutz des Privatlebens.

[19] Pacto de Santa Cruz de La Sierra.

Preocupado em assegurar a privacidade, o art. 21 do Código Civil, dispôs expressamente a respeito da vida privada, constituindo-se em uma cláusula geral para conferir efetividade por meio da norma dogmática, às situações fáticas[20].

3 MUTAÇÕES DA PRIVACIDADE

Diante da exposição exacerbada das pessoas nos dias de hoje, que constantemente tiram fotos e as expõem na rede, bem como veiculam opiniões a respeito dos mais diversos assuntos, pergunta-se: a privacidade acabou? Quais as suas consequências e limites, na esfera virtual e na esfera da denominada vida real?

Importantes autores fazem reflexões destas consequências na seara jurídica, como a seguir se verá. Trabalhar-se-á, principalmente com marco teórico, no tocante à (in)existência da privacidade, frente ao fenômeno informático, composto pelo trio de autores importantes, que se ocupam desta problemática: Antonio-Enrique Pérez Luño, Stefano Rodotá e Manuel Castells. Em uma síntese apertada: Pérez Luño propugna a Metamorfose da Privacidade, Rodotà a Reinvenção da Privacidade e Manuel Castells atualiza o simbolismo do Panótico, e diz que se vive sob a vigilância de um Panótico eletrônico, afirmando que a privacidade deixará de existir nas relações virtuais.

Pérez Luño designa *metamorfose da intimidade*[21]. Uma metamorfose no direito à intimidade que se expressa duplamente: do original direito a estar só individualmente à perspectiva de estar no âmbito social e coletivo; e desde o direito à personalidade ao deslocamento que aponta para órbita patrimonial[22].

---

[20] CACHAPUZ, Maria Cláudia. *Intimidade e vida privada no novo Código Civil Brasileiro*: uma leitura orientada no discurso jurídico. Porto Alegre: Fabris, 2006, p. 213.

[21] PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012, p. 115.

[22] A respeito da evolução do direito à intimidade, veja-se artigo produzido no Anuário nº 10 da Unisinos. LIMBERGER, Têmis. *Acesso à informação pública em rede: a construção da decisão adequada constitucionalmente*. In: Lenio Luiz Streck; Leonel Severo Rocha; Wilson Engelmann. (Org.). Constituição, sistemas sociais e hermenêutica. Anuário do Programa de Pós-Graduação em Direito da Unisinos. 1ed. Porto Alegre e São Leopoldo: Livraria do Advogado e Unisinos, 2013, p. 259/276.

O primeiro significado da intimidade (direito a estar só) se situa na esfera de *foro interno*, de solidão, de ensimesmamento e autoconfinamento pessoal, consequentemente, este conceito corre o risco de ser inexplicável e carecer de qualquer relevância jurídica; ou se ao contrário, toma-se como ponto de referência suas implicações e projeções intersubjetivas no âmbito do "foro externo", corre-se o risco de deformar a intimidade, de coisificá-la, de dilui-la em um conjunto de tópicos sociais, e vendê-la em seu antônimo, isto é, na sua alteração; ou seja, em que deixe de ser ela mesma para ser traída, levada e tiranizada pelo outro[23].

Existe algum ponto de mediação nesta polaridade do dilema, aparentemente insolúvel? Antonio Enrique Pérez Luño estima que sim. A concepção de intimidade como isolamento e ensimesmamento não é necessariamente incompatível com suas projeções sociais, caso se coloque como um primeiro momento de seu processo formativo. Esse *intus* ou fase solitária e interna da intimidade se encontraria conformada por ideias, que reclamariam sua posterior exteriorização em ações. O isolamento confinado em si mesmo somente seria capaz de fabricar mundos exteriores, fantasmagóricos condenados a degenerar em puro solipsismo. A dimensão interna e ensimesmada da intimidade para realizar-se plenamente precisa extroverter-se; a convivência é indispensável na nossa vida, necessita apoiar-se em outras vidas[24].

Essa abertura da convivência se exercita por formas de comunicação e de linguagem que se integram e socializam no mais íntimo de nosso ser, assim o ser mais íntimo de cada homem já está informado, modelado por uma determinada sociedade. Isto porque, a

---

[23] ORTEGA Y GASSET, J. *El hombre y la gente* , en Obras Completas, Alianza Editorial & Revista de Occidente, vol.7, Madrid, 1983, *apud* PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012, p. 116.

[24] GARCÍA MORENTE, *Ensayo sobre la vida privada* (1935); se cita por la nueva Ed. De la Facultad de Filosofía de la Universidad Complutense, Madrid, 1992, p. 36, "*apud*" PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012, p.116.

própria noção de intimidade ou de privacidade é uma categoria cultural, social e histórica[25].

Assim, o núcleo significativo da intimidade se deslocou, inclusive se pode afirmar que foi ao seu oposto, desde o âmbito solitário do ensimesmamento à esfera dos usos sociais em que se manifesta e se exterioriza em termos de alteração. A decantação da cultura europeia da intimidade e privacidade, que pretende traduzir a noção anglo-saxão de privacidade, assim como a categoria dos denominados dados pessoais e perfis de personalidade, que se projetam sobre um conjunto mais amplo e global das relações intersubjetivas, refletem esta tendência paradoxal em direção a uma *socialização da intimidade*[26].

Outro aspecto que merece referência é o fato de que houve um deslocamento do âmbito do direito de personalidade ao âmbito patrimonial, considerando que muitas pessoas recebem quantias patrimoniais expressivas para exporem sua intimidade, negociando esta exposição, principalmente em programas televisivos[27].

Dentre as contribuições de Savigny está a noção de direito de personalidade, possivelmente alicerçada na filosofia jurídica Kantiana[28]. Um conceito de dignidade humana como valor fundamental das noções de pessoa e personalidade, propôs Kant. A dignidade implica, a dimensão moral de personalidade, que tem como fundamento a própria

---

25 ORTEGA Y GASSET, J. *El hombre y la gente* , en Obras Completas, Alianza Editorial & Revista de Occidente, vol.7, Madrid, 1983, *apud* PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012, p. 116.

26 CABEZUELO ARENAS, A.L. *Derecho a la intimidad*, con Prólogo de L. H. CLAVERÍA GOSÁLBEZ, Tirant to Blanch, Valencia, 1998; CLAVERÍA GOSÁLBEZ, L. H., Reflexiones sobre los derechos de la personalidad a la luz de la LO1/82 de 5 de mayo de 1982, em *Anuario de Derecho Civil,* octubre-deciembre, 1983, pp. 1243/1268; M. GALÁN JUAREZ, *Intimidad, Nuevas dimensiones de un nuevo derecho,* Editorial Universitaria Ramón Areces & Servicio de Publicaciones de la Universidad Rey Juan Carlos I, Madrid, 2005, p. 79 ss.; PÉREZ LUÑO, A. E., Intimidad y protección de datos personales: del habeas corpus al habeas data, en *Estudios sobre el derecho a la intimidad,* ed. A cargo de L. GARCÍA SAN MIGUEL, 1982, cit., Tecnos, Madrid, 1992, p. 36 ss.; id., *Libertad informática y leyes de protección de datos personales,* en colab. Con M.G. LOSANGO y M.F. GUERRERO MATEUS, Centro de Estudios Constitucionales, Madrid, 1989.

27 Programa televisivo exibido por emissora nacional denominado *Big Brother Brasil.*

28 PREUSS, U., *Die Internalisierung des Subjekts. Zur Kritik der Funktionsqeise des subjektiven Rechts,* Surhrkamp, Frankfurt, 1979, p. 21 ss.

liberdade e autonomia da pessoa. Aí que a dignidade humana representa o princípio legitimador dos denominados direitos de personalidade.

A intimidade, que foi concebida inicialmente, como integrante dos direitos de personalidade e um dos mais destacados exemplos; atualmente, com os novos perfis coletivos e sociais, que conformam o exercício do direito à intimidade, encontra-se condicionada aos acontecimentos sociais. Com isso, a intimidade corre o risco de ser submetida aos modismos e, inclusive, às exigências de mercado.

Por isso, na sociedade da informação e de consumo, a intimidade se converteu, em muitas ocasiões, em uma mercadoria cujo valor se calcula em termos da lei da oferta e da procura. Nestas ocasiões, a intimidade de cada um vale o que os demais, em especial os meios de comunicação estão dispostos a pagar para publicizá-la[29] .

Diante deste quadro, pergunta-se: o que tem valor? O que as pessoas estão dispostas a pagar para inteirar-se com relação à vida dos demais? Porque o interesse das pessoas na vida alheia, não é facilmente perceptível, fica submetido às leis de mercado[30]. Quando houver interesse pela divulgação de algo, estarão dispostos a pagá-lo. Assim, percebe-se que estas modificações práticas têm relavância na esfera jurídica e levam ao seu deslocamento, desde a órbita dos direitos de personalidade aos direitos de conteúdo patrimonial.

Deste modo, o direito à intimidade somente se mantém como direito da personalidade dotado dos atributos de inviolabilidade, irrenunciabilidade e inalienabilidade para os menores, enquanto que para os maiores pode ser objeto de transações consentidas, de renúncias e cessões, em troca das correspondentes prestações econômicas. Constata-se, então, que para os adultos perdeu sua dimensão de direito da personalidade para integrar-se no sistema de direitos patrimoniais[31].

Assim, a metamorfose do direito à privacidade, segundo Pérez Luño, trouxe mudanças importantes. Deslocou-se do âmbito interno -

---

[29] PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012, p. 120.

[30] GARCÍA SAN MIGUEL, L. *Estudios sobre el derecho a la intimidad*, in PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012, p. 120.

[31] PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012, p. 121.

direito a estar só a uma perspectiva social e coletiva e da condição de integrante de direito da personalidade passou a direito patrimonial, porque integra a ótica negocial para muitas pessoas, na condição desfrutada pela maioridade, subsistindo apenas para os menores.

A *reinvenção da privacidade* é como o Rodotà[32] denomina o fenômeno atual, enquanto a construção da identidade, efetua-se em condições de dependência crescente do exterior. Nesta perspectiva, assume um novo significado a liberdade de expressão como elemento essencial da pessoa e de sua situação na sociedade. Isto modifica a relação entre esfera pública e privada e a própria noção de privacidade. Reforça-se a noção de cidadania com outros poderes que caracterizam a cidadania do novo milênio, a partir da constitucionalização da pessoa humana.

Quando se consideram as questões suscitadas pela inovação tecnológica, ocorre o denominado *tsunami digital*[33]. Como consequência desta transformação, o critério de segurança pública se converte em exclusivo critério de referência.

Isto significa que as pessoas estão cada vez mais transparentes e os organismos públicos mais afastados do controle jurídico e político, ocasionando uma nova distribuição de poderes políticos e sociais.

O denominado *tsunami digital* pode ser considerado desde outros pontos de vista, começando pela identidade. Nesta perspectiva, o direito de acesso aos dados representa um aliado forte, em termos de proteção jurídica, que permite manter o controle sobre as próprias informações, seja qual for o sujeito que as gestiona, o local em que se encontrem e as modalidades de sua utilização. Direito fundamental à construção da identidade, já que confere poder para cancelamento nos seguintes casos: dados falsos, ilegitimamente recolhidos, conservados muito além do tempo previsto, os inexatos ou para completação.

O conhece-te a ti mesmo, já não é uma operação voltada ao interior, mas devido a esta nova perspectiva, vai-se ao exterior e à suposta necessidade de conhecer quem somos na dimensão eletrônica, aonde se

---

[32] RODOTÀ, Stefano. *El derecho a tener derechos*. Madrid: Trotta, 2014, p. 293.

[33] The Future Group: Freedom, Security, Privacy: European Home Affaires in na Open World, junho de 2008, In RODOTÀ, Stefano. *El derecho a tener derechos*. Madrid: Trotta, 2014, p.298.

desenvolvem questões importantes nas nossas vidas. Considerando hoje a dinâmica que caracteriza a recolhida dos dados e os sujeitos que a utilizam, cada vez é menos verossímil uma identidade como *sou o que digo que sou*, pois que haveria que substituí-la por *tu és o que Google diz que és*[34].

Por isso, Eliser Pariser[35] abordando o que você quer, quer queira, quer não, trabalha a questão hipotética ou real, mas que se constitui em ótimo exemplo de seu interesse por uma moça de determinado perfil e com uma foto postada. Surpreendentemente descobriu que a imagem não era sequer uma fotografia editada, mas uma imagem criada por um programa gráfico *3D*. Aquela pessoa não existia, a nova possível amiga, era uma criação de *software*, que ia em busca das ditas novas amizades e que, em realidade, recolhia dados de usuários no *facebook*.

Vive-se diante de um contexto que afeta nossa autonomia e o direito de desenvolver livremente nossa personalidade. Diminui-se a possibilidade de nos conhecermos e nos construirmos. Faz-se mais forte a possibilidade de que outros se apropriem total ou parcialmente do nosso ser.

O propósito de estar *on line* com a vida real. Autenticidade e transparência e - não intervenção e anonimato - são regras fundamentais na internet.

A construção da identidade fica entregue por completo aos algoritmos. A construção da identidade é interior e exterior. O sistema deve então: a) fazer explícito o fluxo de dados para permitir o controle da pessoa interessada, b) respeitar o princípio da minimização dos dados, tratando somente aqueles necessários em um contexto determinado, c) impor limites às conexões entre bancos de dados.

Devido à justificativa do *11 de setembro*, cada vez mais se invade a privacidade por motivos de segurança. Tudo está articulado não para exaltar a pessoa humana e sua singularidade e autonomia, senão para depositar dados em dispositivos tecnológicos, que prescindem de singularidades e de liberdades. A construção dos perfis individuais, familiares e de grupos constitui uma jaula mais repressora que o *status*.

---

[34] RODOTÀ, Stefano. *El derecho a tener derechos*. Madrid: Trotta, 2014, p. 300.

[35] PARISER, Eli. *O filtro invisível: O que a internet está escondendo de você*. Zahar: Rio de Janeiro, 2011, p. 169.

A autodeterminação se torna irrelevante face à identidade esculpida mediante procedimentos automáticos. A nova abstração produz um esvaziamento do humano, de modo que é problemático afirmar que nos encontramos frente a uma nova antropologia.

Manuel Castells[36] - um dos maiores sociólogos da atualidade no estudo das redes sociais e internet - adverte para o perigo da exposição exacerbada nas redes, os programas de vigilância governamentais. Chega a afirmar de forma contundente que a privacidade na rede mundial de computadores acabou, no denominado mundo virtual. Apesar do gasto de bilhões de dólares em segurança eletrônica, tornou-se evidente, que numa rede, a segurança só é tão boa, quando a segurança do elo mais fraco está protegida. Penetrando-se na rede, em qualquer ponto, pode-se percorrer seus nós com relativa facilidade.

A comunicação continuará fluindo imperturbável porque esta é a arquitetura da internet. É necessário, então, que o Estado exerça algum controle e regulamente o ciberespaço. Deste processo, existem duas vítimas dessa retomada do ciberespaço: a soberania e a liberdade. Para exercer a regulação global, os Estados têm de difundir e compartilhar poder. Não segundo o sonho ultrapassado de um governo mundial, mas como um Estado em rede, criatura política engendrada pela Era da Informação (Carnoy e Castells).

Isto envolve a (in)capacidade que tem um Estado de agir sobre um comportamento, que tem lugar em outra jurisdição – isso será limitado pelas velhas formas de poder baseadas na territorialidade.

Castells adverte a respeito do *Panóptico Eletrônico*[37]. Há uma ameaça fundamental à liberdade sob o novo ambiente de policiamento global: a estruturação do comportamento cotidiano pelas normas dominantes da sociedade. A liberdade de expressão era a essência do direito à comunicação irrestrita na época em que a maior parte das atividades diárias não era relacionada à esfera pública. Mas em nosso tempo, uma proporção significativa da vida cotidiana, inclusive o trabalho, o lazer, a interação pessoal, tem lugar na Internet. A maior parte

---

[36] CASTELLS, Manuel. *A Galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade*. Rio de janeiro: Zahar, 2003, p. 145 e 152.

[37] CASTELLS, Manuel. *A Galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade*. Rio de janeiro: Zahar, 2003, p.148.

da atividade econômica, social e política é de fato um híbrido de interação on-line e física. Em muitos casos, estão imbricadas. Assim, viver num panóptico eletrônico equivale a ter metade de nossas vidas permanentemente expostas a monitoramento.

A segunda perda é a liberdade; isto é, o direito de se fazer o que se quer. Por que isso? Por que a ameaça à privacidade traduz-se na redução potencial de liberdade?

Destarte, é impossível conceber direitos e garantias tendo como referência espaços do passado, especialmente nas dinâmicas sociais, no que diz respeito ao direito à intimidade.

4 FUNDAMENTOS DO DIREITO AO ESQUECIMENTO

O direito se constrói conectado com a evolução da sociedade, por isto os institutos de segurança jurídica assentam bases nas relações sociais, constituindo-se em episódios narrados na literatura e estudados pela filosofia.

Livro emblemático que discutiu a invasão da privacidade pelo Estado Totalitário foi 1984[38], uma alusão ao futuro, porque foi escrito no ano de 1948. O Big Brother descrito por Orwell[39], ocupa-se de manipular o passado. O ditador Orwelliano compreendeu que seu poder somente seria total no dia em que pudesse reescrever o passado a seu favor. Assim, por meio do Ministério da Verdade estabeleceu funcionários guardiões de arquivos, cuja tarefa consistia em atualizar minuto a minuto o passado e apagar todos os traços que pudessem dificultar o poder hoje, revelando, principalmente, suas prevaricações e alianças em busca do poder.

A ideia de que os fatos devem ter um tempo de apreciação é algo já conhecido pelo ordenamento jurídico. A legalidade e a segurança jurídica convivem como princípios em nosso ordenamento jurídico. Por vezes, tem-se um determinado princípio com aplicação preponderante ora outro, a depender dos casos enfrentados.

---

[38] ORWELL, George. *1984*. 29. ed., São Paulo: Editora Nacional, 2003, p. 24.

[39] ORWELL, George. *1984*. 29. ed., São Paulo: Editora Nacional, 2003, p. 62/3. "A história seria inteiramente um palimpsesto raspado e reescrito tantas vezes quanto necessárias".

A legalidade é o grande princípio estruturante do ordenamento jurídico, principalmente no direito público, a partir de sua formação, tomando-se como marco a Revolução Francesa em 1789; mas ocorrem situações em que cede passo à segurança jurídica (mormente nas suas manifestações de Coisa Julgada, Ato Jurídico Perfeito e Direito Adquirido previstas pelo artigo 5º, XXXVI da CF).

Deve-se atentar que o princípio da segurança jurídica prepondera sobre o princípio da legalidade, quando o destinatário do ato estava de boa-fé. O direito alemão teve a primazia na formulação deste conceito. Posteriormente, este ensinamento foi expandido ao direito comunitário[40]. No Brasil, a incorporação legislativa ocorreu por meio dos artigos 2º, "caput", e 53 da Lei nº 9.784/99 (Lei do Processo Administrativo no âmbito Federal).

Além disso, os institutos da prescrição, decadência, perdão, anistia, irretroatividade da lei, prazo máximo para que os inadimplentes figurem em cadastros restritivos de crédito, reabilitação penal e o direito ao sigilo quanto à folha de antecedentes, relativo àqueles que já cumpriram pena são exemplificações de que existe um tempo em que os fatos devem ser lembrados para produzir efeitos jurídicos e a partir de determinado momento deixam de sê-lo. Configura-se, em realidade, um embate entre o privilegiamento do passado ou o presente com a perspectiva de futuro.

A respeito do tempo presente - como o que existe em realidade - sendo aquele que nos é dado viver, estatui Schopenhauer: A forma de aparecimento da vontade é só o presente, não o passado nem o futuro: estes só existem para o conceito e pelo encadeamento da consciência, submetida ao princípio da razão. Ninguém viveu o passado, ninguém viverá o futuro; *o presente é a forma de toda a vida*[41].

Assim, para viver o presente não se pode estar demasiado vinculado com o passado e nem tampouco com a mente conectada extremamente ao futuro. Os tempos se influenciam, reciprocamente, na

---

[40] COUTO E SILVA, Almiro do. *O Princípio da Segurança Jurídica (proteção à confiança) no direito público brasileiro e o direito da administração pública de anular seus próprios atos administrativos*: o prazo decadencial do art.54 da Lei do Processo Administrativo da União (Lei nº 9.784/99). RDA, Rio de Janeiro: 2004.

[41] SCHOPENHAUER. *O Mundo como vontade e representação*, Primeiro Tomo, p. 54. (Borges, vol.1, p. 436)

tomada de decisão, mas é necessário que se esteja com foco na perspectiva atual, do tempo presente.

A respeito da impossibilidade humana de recordar todos os fatos, a literatura já se ocupou. Borges escreveu um conto denominado: Funes, o Memorioso. Aí o autor narra o personagem Funes que lembrava absolutamente todos os detalhes na composição de uma narração e o transtorno que isto lhe causava. *Mais recordações tenho eu sozinho que as que tiveram todos os homens desde que o mundo é mundo*. (...) *Minha memória, senhor, é como despejadouro de lixos*[42]. Assim, informações em excesso podem comprometer a vida no presente, pois a narrativa inclui todas as representações até então existentes. Deste modo, um simples relato pode consumir todo um dia em sua narrativa, devido a todas as recordações pretéritas.

Caso se recorde absolutamente todos os fatos do passado, isto comprometeria o tempo presente. A memória humana ficaria repleta de informações pretéritas sem possibilitar a construção do tempo presente. Por isso, do ponto de vista jurídico, também se estatui um tempo para que as informações sejam armazenadas. Senão, se estaria eternamente preso ao passado.

Ligar e desligar o tempo; a obra de Ost – O tempo no direito[43], origina-se deste projeto. Qual seja: a contribuição do direito para esta justa medida que torna livre os cidadãos e harmoniosas as cidades. Por meio da perspectiva do passado: a memória e o perdão; por parte do futuro: a promessa e a retomada da discussão. A memória que liga o passado, garantindo-lhe um registro, uma fundação e uma transmissão. O perdão, que desliga o passado, imprimindo um sentido novo, portador de futuro, como quando ao término de uma reviravolta de jurisprudência, o juiz se libera de uma linhagem de precedentes ultrapassados. A promessa, que liga o futuro por meio dos comprometimentos normativos, desde a convenção individual até a Constituição - promessa que a nação faz a si própria. O questionamento, que em tempo útil desliga o futuro, visando operar as revisões que se

---

[42] BORGES, Jorge Luis. *Obras Completas*, volume 1. São Paulo: Globo, 2001, p.543. "In" Ficções – Funes, o Memorioso, pp. 539/546.

[43] OST, François. *O tempo do Direito*. Lisboa: Piaget, 1999.

impõem, para que se sobreponham as promessas na hora da mudança. Para Ost são quatro pontos cardeais do quadrante temporal.

Assim, não é suficiente dizer que memória, perdão, promessa e questionamento estão comprometidos nas relações dialéticas. É preciso ir mais longe e mostrar que é no próprio seio de cada uma delas que se opera a dialética. Há muito de esquecimento na memória e muito de memória no perdão; do mesmo modo, há muito de indeterminação na promessa e muito de fidelidade na revisão. Não existe uma das figuras temporais que reencontraremos, que não ofereça, no mais delicado de seus mecanismos, uma exemplificação desta tensão fecunda entre constância e inovação.

A interação entre o tempo e o direito, que se revela. O tempo metamórfico, no dizer de Gurvitch[44]: tempos de alternância entre avanço e atraso, que sabe se transformar, sem por isso regenerar-se. O temo institucional – nem eterno, nem perecível. O tempo revelador do direito. Nesta revelação, o tempo faz surgir, principalmente, a confiança (boa-fé, lealdade), na base de todos os comprometimentos jurídicos, do mesmo modo que a pertinência institucional do direito – um direito concebido como um processo de ajuste contínuo, mais do que uma sucessão irregular de atos jurídicos instantâneos.

O conhecido *círculo hermenêutico*[45], tem também, a sua dimensão temporal: a troca semântica entre o mundo do texto e o mundo do intérprete é igualmente a reversibilidade histórica em ação, o diálogo entre trechos confusos de respostas formuladas no passado e interrogações expressas no presente.

É importante se insurgir contra a tirania da urgência e a cultura da impaciência, é preciso lembrar que a democracia, sobretudo a participativa, toma seu tempo – o da informação, da negociação e da deliberação. Deve-se atentar contra as tentações da *justiça do espetáculo*[46], em que a mídia insufla a população para que se responsabilize rapidamente um suposto culpado, sem que se atente ao

---

44 GURVITCH, L. *La multiplicité des temps sociaux*. *In* La vocation actuelle de La sociologie. 2ª ed. Paris: PUF, 1963, t.II, . 343 e segs.

45 GADAMER, Hans Georg. *Verdade e método*. v. 1, 10ª ed., Petrópolis/RJ: Ed. Vozes, 2008, p. 166 e ss.

46 OST, François. *O tempo do Direito*. Lisboa: Piaget, 1999.

devido processo legal, que têm seus trâmites e, portanto, leva algum tempo não podendo ser realizado de imediato.

Delmas Marty[47], lembra que o Estado, ao contrário do mercado, tem o privilégio do longo prazo e que, provedor de duração e solidariedade, pode impedir que se rasgue o tecido social no decorrer das mutações que o esquartejam.

Com Hannah Arendt[48] se discorre a respeito do perdão e da promessa. Se o homem não fosse conectado por promessas, seria incapaz de conservar sua identidade, seria condenado a errar sem força e sem objetivo.

Entre a amnésia e o imprescritível: o perdão. Hannah Arendt dedicou muito de seus estudos a respeito do perdão. Este tema foi retomado, posteriormente, na Condição Humana, quando demonstrou que *nunca se pode prever o ato de perdoar*. É a única reação que não se limita a reagir[49], mas age de novo e inesperadamente sem ser condicionada pelo ato que a provocou e de cujas consequências libertam tanto quem perdoa quanto quem é perdoado.

O perdão aposta na liberdade dos interlocutores, vai além do contrassenso do mal e acresce ao sentido. Assim, o ofendido, que por meio de seu gesto imprevisto e gratuito renuncia a reclamar o que lhe é devido, e o ofensor, que se afasta da lógica do nefasto e solicita o perdão e se compromete a restaurar a relação comprometida.

Destarte, o perdão oferece uma nova possibilidade de futuro[50]. A natureza dialética do perdão surge, já que no cômputo total remete à memória (a falta não é esquecida, mas reconhecida e assumida) e, assim, sinaliza com a promessa (a aposta confiante num cenário de futuro).

Diante disto, constitui-se o perdão como uma categoria jurídica? O direito é a mediação do ético e do político, tradução de um na

---

47 DELMAS MARTY, M. *Le maître des horlojes*. Paris: Odile Jacob, 1991.

48 ARENDT, Hannah. *A condição humana*. 10ª ed., Rio de Janeiro: Forense Universitária, 2001, p. 252-3.

49 ARENDT, Hannah. *A condição humana*. 10ª ed., Rio de Janeiro: Forense Universitária, 2001, p. 252-3.

50 RICOEUR, P. Sanction, réhabilitation, pardon. In: *Le juste*, Paris: Ed. Esprit, 1995, p. 207.

linguagem do outro. Desta forma, o perdão, quando conferido no curso de um processo, coaduna-se com a ideia de justiça.

Dois pólos essenciais da regulação jurídica do tempo social[51]: o perdão, em sentido amplo, como a capacidade que tem a sociedade de superar o passado, rompendo o ciclo da vingança e do ressentimento. Por outro lado, a promessa, em sentido amplo, no sentido de crença no futuro - comprometer-se por meio de antecipações normativas.

Deste modo, passado e futuro estão associados a dois atos: o perdão que relança o passado e a promessa, que orienta o futuro, relacionando-se à lei que se coloca frente às incertezas do amanhã. É por isso, que o perdão é associado à memória, enquanto a promessa à retomada da discussão. Assim, opera-se o quadrante em quatro tempos: ligar e desligar o passado e, também, ligar e desligar o futuro. Este o ritmo necessário para uma produção significante do tempo social. O papel de guardião da memória social foi, em todos os tempos, confiada aos juristas[52]. Não no sentido de arquivistas ou conservadores dos atos do passado, mas no sentido de que são seguidores do Princípio da Legalidade. E, ainda, que os operadores jurídicos têm consciência de que só se institui o novo com base no instituído. Sempre há uma parte de indisponível, na medida em que nenhuma instituição é absolutamente nova. Poder-se-ia dizer que o novo assenta suas bases no tecido social cunhado ao longo do tempo.

A prescrição é o esquecimento programado pelo direito[53]. É também, quando ocorre o privilegiamento das situações convalidadas pelo tempo em detrimento da legalidade, que é um princípio estruturante, principalmente na seara do direito público.

Quando aborda o direito ao esquecimento ou dever de memória[54], Ost apresenta duas situações distintas. O anonimato decorrente das técnicas de fertilização assistida, da adoção, em que se objetiva a realização do interesse público. Em outras hipóteses, o direito ao esquecimento, consagrado pela jurisprudência, surge como uma das

---

51 OST, François. *O tempo do Direito*. Lisboa: Piaget, 1999, p. 39.

52 OST, François. *O tempo do Direito*. Lisboa: Piaget, 1999, p. 50.

53 OST, François. *O tempo do Direito*. Lisboa: Piaget, 1999, p. 167.

54 OST, François. *O tempo do Direito*. Lisboa: Piaget, 1999, p. 159.

múltiplas facetas do direito ao respeito à vida privada. Quer seja personagem público ou não, caso tenha sido lançado diante de uma cena e colocado diante dos projetores da atualidade (muitas vezes até penal), do qual se tem direito depois de determinado tempo a recair no esquecimento ou do anonimato, do qual não deveria ter saído.

5 CONSIDERAÇÕES FINAIS

A informação pública em rede, por suas características de flexibilidade, adaptação e ausência de centralidade, pode ser um instrumento eficaz de diminuição de corrupção, pois propicia a visualização de zonas de opacidade, possibilitando o acesso do cidadão ou de agentes públicos a cujas instituições incumbem a atribuição de zelar pelo patrimônio público, a fiscalização e tomada de providências.

A informação pública em rede encontra limite na privacidade do cidadão. O direito à privacidade sofreu mutações, frente ao fenômeno informático, visto que o ser humano se encontra conectado com a rede mundial de computadores – internet. Logo, a informação pública em rede deve estar atenta a estes movimentos e aos limites jurídicos.

A forma de lançamento dos dados deve respeitar a proteção dos dados pessoais. No ordenamento jurídico brasileiro, não se tem um marco regulatório específico da proteção dos dados pessoais, devendo ser realizado a partir do direito de privacidade do cidadão. Deve-se construir uma tutela que proteja além dos dados pessoais, contemplando os sistemas de informática, tal qual construção jurisprudencial realizada pelo Tribunal Constitucional da Alemanha.

Caso se recordem absolutamente todos os fatos do passado, isto comprometeria o tempo presente. A memória humana ficaria repleta de informações pretéritas sem possibilitar a construção do presente com a perspectiva de futuro. Por isto, do ponto de vista jurídico, também é necessário estatuir um tempo para que as informações sejam armazenadas. Passado, presente e futuro se influenciam, reciprocamente, para tomada de decisão, mas é importante que o foco seja na perspectiva atual, momento a partir do qual começarão a incidir os seus efeitos.

REFERÊNCIAS

ARENDT, Hannah. *A condição humana*. 10ª ed., Rio de Janeiro: Forense Universitária, 2001, p. 252-3.

ARENDT, Hannah. *Entre o passado e o futuro*. 6ª ed. São Paulo: Perspectiva, 2009 (Debates; 64/ dirigida por Guinsburg). Que é a liberdade.

BENDA, Ernesto. *Dignidad Humana y derechos de la personalidad*. In: Manual de Derecho Constitucional. Madrid: Marcial Pons, 1996.

BINICHESKI, Paulo Roberto. *Responsabilidade Civil dos Provedores de Internet*. 1ª edição. Curitiba: Juruá. 2011.

BORGES, Jorge Luis. *Obras Completas*, volume 1. São Paulo: Globo, 2001, p.543. "In" Ficções – Funes, o Memorioso.

CABEZUELO ARENAS, A.L. *Derecho a la intimidad*, con Prólogo de L. H. CLAVERÍA GOSÁLBEZ, Tirant to Blanch, Valencia, 1998.

CACHAPUZ, Maria Cláudia. *Intimidade e vida privada no novo Código Civil Brasileiro*: uma leitura orientada no discurso jurídico. Porto Alegre: Fabris, 2006.

CASTELLS, Manuel. *A Galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade*. Rio de janeiro: Zahar, 2003.

CLAVERÍA GOSÁLBEZ, L. H., Reflexiones sobre los derechos de la personalidad a la luz de la LO1/82 de 5 de mayo de 1982, em *Anuario de Derecho Civil,* octubre-deciembre, 1983, pp. 1243/1268.

COSTA JR., Paulo José da. *O direito a estar só: tutela penal da intimidade*. São Paulo: RT, 1970, p. 31, citando HENKEL, Der Strafschutz des Privatlebens.

COUTO E SILVA, Almiro do. *O Princípio da Segurança Jurídica (proteção à confiança) no direito público brasileiro e o direito da administração pública de anular seus próprios atos administrativos*: o prazo decadencial do art.54 da Lei do Processo Administrativo da União (Lei nº 9.784/99). RDA, Rio de Janeiro: 2004.

CUNHA, Antônio Geraldo da. *Dicionário Etmológico da língua portuguesa*, 2ªed, 11ª reimpressão, Rio de Janeiro: Nova Fronteira, 1999.

DAVARA RODRIGUEZ, Miguel Ángel. *Manual de Derecho Informático*. Madrid: Aranzadi, 1993.

DEBORD, Guy. *A sociedade do espetáculo*. Rio de Janeiro: Contraponto, 1997.

DELMAS MARTY, M. *Le maître des horlojes*. Paris: Odile Jacob, 1991.

DENNINGER, E.. *El derecho a la autodeterminación informativa*. In problemas actuales de la documentación y la informática jurídica, PÉREZ LUÑO, Antonio E. (Org.). Madrid: Tecnos, 1987.

DOTTI , René Ariel. *Proteção à vida privada e liberdade de informação*. São Paulo: RT,1980.

GADAMER, Hans Georg. *Verdade e método*. v. 1, 10ª ed., Petrópolis/RJ: Ed. Vozes, 2008.

GARCÍA MORENTE, *Ensayo sobre la vida privada* (1935); se cita por la nueva Ed. De la Facultad de Filosofía de la Universidad Complutense, Madrid, 1992, p. 36, "*apud*" PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012.

GARCÍA SAN MIGUEL, L. *Estudios sobre el derecho a la intimidad*, in PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012.

GURVITCH, L. *La multiplicité des temps sociaux*. *In* La vocation actuelle de La sociologie. 2ª ed. Paris: PUF, 1963, t.II.

HIGUERAS, Manuel Heredero. *La nueva ley alemana de protección de datos*. Boletín de Información del Ministerio de la Justicia, ano XLVI, nº 1630, 1992, p. 1765. RUIZ MIGUEL, Carlos. *La configuración constitucional del derecho a la intimidad*. Madrid: Tecnos, 1995.

HOUAISS, Antônio; FRANCO, Francisco Manoel de Mello; VILLAR, Mauro de Salles. *Dicionário Houaiss da Língua Portuguesa*. Objetiva: Rio de Janeiro, 2009.

LIMBERGER, Têmis. *CIBERTRANSPARÊNCIA: informação pública em rede: a virtualidade e suas repercussões na realidade.*Porto Alegre: Livraria do Advogado, 2016.

LLOSA, Mario Vargas. *A civilização do espetáculo: uma radiografia do nosso tempo e da nossa cultura*. Rio de Janeiro:Objetiva, 2013.

M. GALÁN JUAREZ, *Intimidad, Nuevas dimensiones de un nuevo derecho,* Editorial Universitaria Ramón Areces & Servicio de Publicaciones de la Universidad Rey Juan Carlos I, Madrid, 2005.

MARTINS, Guilherme Magalhães. O direito ao esquecimento na Internet. In: MARTINS, Guilherme Magalhães (Coord.). *Direito privado e internet*. São Paulo: Atlas, 2014. p. 3/28.

MENKE, Fabiano. *A proteção de dados e o novo direito fundamental à garantia de confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão* "in" Direito, Inovação e Tecnologia, vol. I. Coordenadores: Gilmar F. Mendes, Ingo W. Sarlet e Alexandre Z. Coelho, São Paulo: Saraiva, 2015, pp. 205/230.

MONTENEGRO, Antônio Lindberg. *A Internet em suas relações contratuais extracontratuais*. Rio de Janeiro: Lumen Juris, 2003.

MORAES, Maria Celina Bodin de; KONDER, Carlos Nelson. *Dilemas de direito civil-constitucional casos e decisões sobre os novos desafios para a tutela da pessoa humana nas relações existenciais*. Rio de Janeiro: Renovar, 2012.

MURILLO, Pablo Lucas. *El derecho a la autodeterminación informativa*. Madrid: Tecnos, 1990, p. 157-8 (Temas Clave de la Constitución Española) e Informática y protección de datos personales. Cuadernos e Debates, Madrid nº 43, 1993, p. 47-87.

ORTEGA Y GASSET, J. *El hombre y la gente*, en Obras Completas, Alianza Editorial & Revista de Occidente, vol.7, Madrid, 1983, *apud* PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012.

ORWELL, George. *1984*. 29. ed., São Paulo: Editora Nacional, 2003.

OST, François. *O tempo do Direito*. Lisboa: Piaget, 1999.

PARISER, Eli. *O filtro invisível: O que a internet está escondendo de você*. Zahar: Rio de Janeiro, 2011.

PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012.

PÉREZ LUÑO, Antonio Enrique. *Manual de informática y derecho*. Barcelona: Editorial Ariel S.A., 1996.

PÉREZ LUÑO, A. E., Intimidad y protección de datos personales: del habeas corpus al habeas data, en *Estudios sobre el derecho a la intimidad,* ed. A cargo de L. GARCÍA SAN MIGUEL, 1982, cit., Tecnos, Madrid, 1992.

PREUSS, U., *Die Internalisierung des Subjekts. Zur Kritik der Funktionsqeise des subjektiven Rechts,* Surhrkamp, Frankfurt, 1979.

PROSSER, Willian. *Privacy.* Califórnia Law Review, v. 48, n. 3, 1960.

RICOEUR, P. Sanction, réhabilitation, pardon. In: *Le juste*, Paris: Ed. Esprit, 1995.

RODOTÀ, Stefano. *El derecho a tener derechos*. Madrid: Trotta, 2014.

SÁNCHEZ BRAVO, Álvaro A. *Hacia un nuevo marco europeo de protección de datos personales: empoderamiento de los ciudadanos en la sociedad tecnológica*. In: Sociocibernética e Infoética: contribuición a una nueva cultura y praxis jurídica. (Org.) Yarina Amoroso Fernández. 1ed. Habana - Cuba: Editorial UNIJURIS, 2015, v. 1.

SARTORI, Giovanni. *Teoría de la democracia*. Vol. 2. Madrid: Alianza Editorial, 1988.

SCHOPENHAUER. *O Mundo como vontade e representação*, Primeiro Tomo, p. 54. (Borges, vol.1)

STRECK, Lenio Luiz. *Verdade e Consenso: Constituição, hermenêutica e teorias discursivas*. 4ªed., São Paulo: Saraiva, 2011.

UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia*, de 07 de dezembro de 2000. Carta de Nice. Disponível em: <http://www.europarl.europa.eu/charter/default_pt.htm>. Acesso em: 25 mar. 2016.

UNIÃO EUROPEIA. *Jornal Oficial da União Europeia*. Tratado de Lisboa. C 306, 50º ano, 17 de dezembro de 2007. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:FULL:PT:PDF>. Acesso em: 25 mar. 2016.

WARREN, Samuel D.; BRANDEIS, Louis D. *The right to privacy*. Harvard Law Review, vol. IV, nº 5, p. 193-220, Dec., 1890.

LAS CONSECUENCIAS DEL *BREXIT* SOBRE EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES[1]

Alejandro Corral Sastre[2]

1.- Introducción

El 23 de junio de 2016 los ciudadanos de la Unión Europea, al menos aquellos que nos consideramos europeos convencidos, sufrimos un duro golpe. El Reino Unido, uno de los Estados Miembros más antiguos de la Unión[3], decidió, por medio de un referéndum no vinculante, separarse del proyecto europeo.

Desde entonces, todo el proceso ha estado rodeado de mucha incertidumbre: en cuanto a si el Gobierno iba a tener en cuenta el referéndum, dado que no era vinculante; sobre si se notificaría la decisión que daría comienzo al procedimiento del artículo 50 del Tratado de la Unión Europea (en adelante, TUE); acerca del papel que debe jugar el Parlamento Británico en todo el proceso; respecto a la posibilidad de que se celebre un segundo referéndum que anule en anterior; en qué posición quedarían los territorios del Reino Unido que, mayoritariamente, votaron a favor de la permanencia[4]; entre otras muchas cuestiones que quedan en el aire. Todo ello aderezado, además,

[1] El presente trabajo se inscribe en el Proyecto de Investigación sobre *Protección de Datos, Seguridad e Innovación: Retos en un mundo global tras el Reglamento Europeo de Protección de Datos*, Ref. DER2016-79819-R, del programa I+D del Ministerio de Economía y Competitividad del que es investigador principal el Dr. D. José Luis PIÑAR MAÑAS: www.privacidadyacceso.com.

[2] Profesor Colaborador Doctor de Derecho Administrativo. Universidad CEU- San Pablo de Madrid. Abogado

[3] Reino Unido se incorpora a la Unión Europea en 1973 junto con Irlanda y Dinamarca. No es por tanto uno de los Estados Miembros originarios, sino que se incorporó en la primera ampliación. No obstante, debemos señalar que la relación de Reino Unido con la Unión Europea ha sufrido, si se permite la expresión, muchos altibajos a lo largo de su historia.

[4] Según la página web de la BBC los resultados del referendum por territorios son los siguientes*: In England 53.4% of the votes were to leave the EU (15,188,406); in Northern Ireland 44.2% of the votes were to leave (349,442); in Scotland 38.0% of the votes were to leave (854,572)* consultado por última vez el 24 de julio de 2017 en http://www.bbc.com/news/politics/eu_referendum/results

con unas elecciones anticipadas convocadas por la Primera Ministra, Theresa May[5], en las que el partido conservador, lejos de consolidar una posición firme para la futura negociación con la Unión, ha perdido la mayoría absoluta en el Parlamento[6], lo que genera aún más incertidumbre, si cabe, en todo este proceso.

No obstante, y por desgracia para aquellos que aún albergamos ciertas esperanzas sobre la permanencia[7], vemos, con desasosiego, como el Gobierno británico se mantiene firme en su decisión y se están dando los primeros pasos para materializar la salida definitiva. En este sentido, el Gobierno británico notificó su decisión al Consejo Europeo el pasado 29 de marzo en los términos establecido en el apartado segundo del artículo 50 del TUE, ya mencionado, y han empezado las negociaciones de cara a una salida definitiva que se hará efectiva, probablemente, en la primavera de 2019.

En este contexto, es necesario aclarar que este trabajo se basa en hipótesis que todavía no se han materializado, por lo que es posible que en el futuro no se hagan realidad. No obstante, lo considero un ejercicio necesario para situarnos en los diferentes escenarios que pueden darse respecto al derecho fundamental a la protección de datos personales, dado que cuando la salida sea definitiva, el Reino Unido será considerado como un tercer estado a efectos de la aplicación del Reglamento General de Protección de Datos[8] (en adelante, RGPD), es decir, se habrá de tener en cuenta lo dispuesto en el Capítulo V (artículos 44 a 50), que regulan

---

[5] Theresa May llega al cargo tras la Dimisión de David Cameron, precisamente, tras los resultados del referéndum.

[6] El sistema electoral británico se basa en el *first-past-the-post*, es decir, "*On polling day, the ballot paper is made up of candidates who are members of parties or independents. As only one MP will get elected, each party only stands one candidate to chose from. Voters put a cross next to their favourite candidate, or the candidate they like they most who they think has the best chance of winning*", en este sentido, véase: www.electoral-reform.org.uk

[7] En este sentido, MARTÍN DELGADO, I., "Brexit means Brexit… o no. Especulaciones, conjeturas y algunas consideraciones jurídicas al propósito de la decisión del Reino Unido de retirarse de la Unión Europea en el contexto del artículo 50 del TUE", *El Cronista del Estado Social y Democrático de Derecho*, núm. 64. No obstante, y aun a riesgo de caer en un optimismo imprudente, se ven ciertos atisbos de esperanza en declaraciones como las del nuevo líder del partido liberaldemócrata, Vince Cable, quien abandera el movimiento *antibrexit*.

[8] A estos efectos, Reino Unido no pertenecerá tampoco, al menos en principio, al Espacio Económico Europeo del que forman parte Islandia, Liechtenstein y Noruega.

las "transferencias internacionales de datos personales a terceros países u organizaciones internacionales", así como los correspondientes considerandos (del 101 al 116) que adquieren, como se verá, especial importancia.

Pero antes de referirnos a las consecuencias de *Brexit* sobre el derecho fundamental a la protección de datos, es necesario, según estimo, hacer referencia, si quiera breve, al contexto en que se produce la votación en el referéndum

2.- Breve referencia al contexto económico, político y social en el Reino Unido del *Brexit*.

Para realizar un esbozo aproximado de las consecuencias de la salida del Reino Unido de la Unión Europea, debemos acercarnos a las causas que lo provocaron. Es decir, por qué una muy reducida mayoría de ciudadanos británicos votaron a favor del *Brexit*[9].

En primer lugar, parece que los ciudadanos del Reino Unido no votaron con toda la información sobre las posibles consecuencias económicas de la salida. Así, algunos autores plantean que mucha información relevante fue deliberadamente escondida a los votantes[10], lo

[9] Como es conocido, la votación al favor de la salida de la Unión Europea se impuso por muy poco: Votos a favor del *Brexit*: 17.410.742 (51,9%) Votos a favor de permanecer: 16.577.342 (48,1%) Total de votos: 33.577.342 Participación: 72%. http://www.bbc.com

[10] WELFENS, P. J. J., "Cameron's information disaster in the referendum of 2016: an exit from Brexit?", *International Economics and Economic Policy*, octobre, 2016, pág., 540, "*Prime Minister Cameron had not managed to include extremely important information on the economic effects of a BREXIT, from a study by the Treasury (HM Government 2016a) published on 18th April, 2016, in the 16-page info booklet (HM Government 2016b) which was sent out to all households: between 11th and 13th April to all households in England, and during the week from 8th May to all households in Scotland, Wales and Northern Ireland. The 6.2 % reduction in income as a long-term consequence of BREXIT, which Chancellor of the Exchequer George Osborne stressed in the press release on the 18th April, remained a fact hidden from the vast majority of households. If one takes into consideration the usual links between income trends and voting results in opinion polls/national elections and assumes a similar influencing factor in the case of a referendum, the BREXIT referendum would actually have resulted in a victory for the Remain camp had this information been more widely known. The Cameron government allowed the overwhelming majority of voters to cast their vote under a veil of ignorance regarding the economic consequences of a UK exit from the EU; a phenomenon which is historically unique. On the other hand, the Cameron government proved itself capable, when the situation of the referendum on Scottish independence arose in 2014, i.e. the preservation of the United Kingdom, of supplying all Scottish households with the relevant economic information, by providing two economically*

que no puede ser considerado democrático, teniendo en cuenta la trascendencia de la votación, no solo para los ciudadanos británicos.

Pero si se analiza más en profundidad, hay un trasfondo social y político que no se puede desdeñar[11]. Así, parece que una de las principales razones que llevó a muchos ciudadanos a votar a favor de la salida fue la inmigración. Es decir, los ciudadanos británicos perciben que hay un exceso de inmigrantes y que ello se debe, fundamentalmente, a las políticas que se aprueban desde la "lejana" Bruselas, donde no se tienen en cuenta los problemas reales de los británicos[12].

Por otro lado, no se puede negar que el *Brexit* es una consecuencia, casi inmediata, de la grave crisis económica mundial que se ha vivido en los últimos años. Los ciudadanos de clase media y trabajadores de todo el mundo han percibido que las políticas que se impulsan desde la Unión Europea, políticas en definitiva basadas en la globalización de la economía, lejos de beneficiarles, han contribuido a empeorar su situación y a mermar sus derechos sociales. Parece ser, por consiguiente, que el ciudadano medio del Reino Unido ha dado un voto de castigo a aquellos que, según su idea, realmente se benefician con la pertenencia del Reino Unido a la Unión: los trabajadores del sector financiero de la *City*[13].

La situación económica y social del Reino Unido ha sido el caldo de cultivo idóneo para que surjan movimientos populistas de corte iliberal, es decir, partidos políticos que defienden un patriotismo excluyente y xenófobo[14]. Además, la crisis de los refugiados sirios y los

---

convincing info brochures to all households in Scotland, which contained meaningful insights on the expected consequences of a vote for Scottish independence according to experts, in a timely manner. Against this background, the 2016 referendum therefore appears as damaging to democratic quality standards and thus unfair to British voters and EU partner countries alike"

[11] CRAIG, P., "*Brexit: A Drama in Six Acts", European law review,* núm. 4, 2016, págs. 447-468

[12] SARMIENTO, D., "Y después del Brexit… ¿Qué?", *El Cronista del Estado Social y Democrático de Derecho*, núm. 64, pág. 42.

[13] JAMES, S., y QUAGLIA, L., "*The political economy of finance in the UK and Brexit*", en *The Political Economy of Brexit and the UK's National Business Model*, SPERI Paper No. 41, 2017, págs. 7 a 10.

[14] Me refiero fundamentalmente al Partido por la Independencia del Reino Unido, o *United Kingdom Independence Party* o *UKIP*, que realizaron una intensa campaña a favor de la salida de la Unión Europea.

atentados terroristas sufridos en los últimos meses han alentado esta idea que, en definitiva, ha propiciado el resultado del referéndum.

Sirva esta lección para que no se vuelva a producir una situación semejante en otro Estado Miembro de la Unión Europea, pues como señala Daniel SARMIENTO, "Actuar como si la retirada del Reino Unido fuese únicamente una cuestión interna británica sería un planteamiento tan suicida como el de la orquesta del Titanic. La Unión debe realizar un proceso de reflexión no tanto para pensar el RU, sino en sí misma, so pena del que el *Brexit* sea el catalizador de un imparable efecto dominó que termine desbaratando el proyecto de integración europea en su totalidad"[15]

3.- El Reglamento General de Protección de Datos y el proceso de salida del Reino Unido de la Unión Europea.

En este contexto al que se acaba de hacer referencia, lo único que se puede saber con certeza es cuando será aplicable el RGPD. Como es sabido, el Reglamento se publicó en el Diario Oficial de la Unión Europea (en adelante, DOUE) el 4 de mayo de 2016. Su artículo 99 establece dos periodos distintos: entrada en vigor, por un lado, y aplicación, por otro. Es decir, una cosa es que el RGPD haya entrado ya en vigor a los 20 días de su publicación en el DOUE, y otra, bien diferente, es que sea aplicable. Por tanto, pese a que esté en vigor desde el 24 de mayo de 2016, no podrá exigirse su aplicación en los Estados Miembros, hasta el 25 de mayo de 2018, en los términos establecidos en el apartado 2 del artículo 99. En este sentido, y para que los Estados Miembros puedan adaptarse convenientemente a las novedades que incluye la nueva regulación, se otorga un periodo de dos años en los que, pese a estar en vigor, el RGPD no es aplicable[16].

---

[15] SARMIENTO, D., "Y después del Brexit… ¿Qué?", *op. cit.,* pág. 44.

[16] En este sentido, véase TORREGROSA VÁZQUEZ, J., "Revisión de otros actos jurídicos de la Unión en materia de Protección de Datos, entrada en vigor y aplicación del Reglamento", en PIÑAR MAÑAS, J. L. (Director), y ÁLVAREZ CARO M., y RECIO GAYO, M., (Coordinadores), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, pág. 681, "Sin entrar en el nada desdeñable debate sobre la diferenciación entre la entrada en vigor y la aplicabilidad de

Este periodo de adaptación a la nueva regulación sobre protección de datos coincide, como es fácilmente comprensible, con el proceso de salida del Reino Unido de la Unión Europea. Así, habrá que determinar los diferentes escenarios hipotéticos que puedan producirse durante todo este periodo. A ellos me referiré más adelante.

4.- La regulación de las transferencias internacionales de datos en el RGPD

Si se tienen en cuenta que, tras el *Brexit*, el Reino Unido será considerado un tercer estado a efectos del tratamiento de datos personales, se ha de indicar, aunque sea muy brevemente, como se regulan las trasferencias internacionales de datos en el RGPD, pues existe alguna novedad respecto al régimen jurídico establecido en 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 (en adelante, la Directiva o Directiva 95/46)[17].

Sobre lo que deba ser considerado transferencia internacional, lo cierto es que el RGPD no lo establece. Tampoco lo hacía la Directiva[18]. Una definición de transferencia internacional la encontramos en el artículo 12 del Convenio 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, donde se indica que son transmisiones de datos "a través de fronteras nacionales"[19]. Por otro lado,

---

las normas, es conveniente anotar que el legislador ha optado por implantar una comprensible etapa de transición de dos años hasta su aplicación"

[17] Según el artículo 94 del RGPD la Directiva queda derogada con efecto a partir del 25 de mayo de 2018, es decir, está derogada, pero sigue teniendo efectos. Es una consecuencia más del peculiar sistema de entrada en vigor del Reglamento.

[18] Así lo pone de manifiesto PIÑAR MAÑAS, J.L., "Transferencias de datos personales a terceros países u organizaciones internacionales" en PIÑAR MAÑAS, J. L. (Director), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, op. cit.,* pág. 431.

[19] REMOLINA, N., *Recolección internacional de datos personales: un reto del mundo post-internet*, edición conjunta de la Agencia Española de Protección de Datos y la Agencia Estatal Boletín Oficial del Estado, Madrid, 2014, págs. 170 a 172

podemos acudir a la definición que nos ofrece nuestro ordenamiento interno en 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 adelante, RLOPD), en vigor, en cuyo artículo 5.1.s), dedicado a definiciones, señala que una transferencia internacional de datos es un: "Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español"[20]. Es decir, transferencia internacional se producirá cuando haya un tratamiento de datos fuera del Espacio Económico Europeo (en adelante, EEE).[21]

Se trata, en cualquier caso, de una definición compleja y habrá que estar, en cada momento, a lo que establezca la jurisprudencia del Tribunal de Justicia de la Unión Europea. Parece, no obstante, que el concepto de transferencia internacional puede ampliarse a aquellos supuestos en los que no solo haya un envío de información, sino también una puesta a disposición de los datos para su consulta[22].

4.1.- Breve referencia a las transferencias internacionales de datos en la Directiva 95/46.

La regulación de las transferencias internacionales de datos en la Directiva se encontraba en los artículos 25 y 26. Según estos preceptos, solo era posible realizar una transferencia internacional de datos cuando

---

[20] GUASCH PORRAS, V., *Las transferencias internacionales de datos en la normativa española y comunitaria*, edición conjunta de la Agencia Española de Protección de Datos y la Agencia Estatal Boletín Oficial del Estado, Madrid, 2014, págs. 46 a 48.

[21] Como es sabido, el Espacio Económico Europeo se instauró el 1 de enero de 1994 con motivo de un acuerdo entre países miembros de la Unión Europea y de la Asociación Europea de Libre Comercio (AELC), excepto Suiza. Su creación permitió a los países de la AELC participar en el mercado interior de la Unión Europea sin tener que adherirse a la UE. Los miembros son los 28 (27 tras el *Brexit*) países integrantes de la UE y los miembros de la AELC siguientes: Islandia, Liechtenstein y Noruega.

[22] PIÑAR MAÑAS, J.L., "Transferencias de datos personales a terceros países u organizaciones internacionales" en PIÑAR MAÑAS, J. L. (Director), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, op. cit.,* pág. 433

el país tercero correspondiente garantizara un nivel de protección adecuado (artículo 25). Esa era, por tanto, la regla general. Sin embargo, el artículo 26 reconocía un amplio elenco de excepciones, entre las que cabía destacar, en lo que ahora interesa, la reconocida en su apartado segundo, es decir, que el Estado Miembro podía autorizar una transferencia a un tercer país que no gozara de un nivel adecuado de protección, cuando el responsable de tratamiento ofreciera garantías suficientes de que los derechos de las personas fueran adecuada y suficientemente protegidos[23].

[23] Artículo 26

Excepciones

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

Como veremos en los apartados siguientes, esa excepción a la que se acaba de hacer referencia, se ha convertido, con el RGPD, en regla general.

4.2.- La regulación de las transferencias internacionales de datos según el RGPD.

Lo primero que cabe destacar, respecto a la nueva regulación, es el sensible incremento de artículos referidos a las transferencias internacionales, lo que pone de manifiesto la importancia de la cuestión[24]. Así, de dos artículos que dedicaba la Directiva, se pasa a seis en el RGPD, muy extensos, además: del 44 al 49.

También es reseñable que mientras en la Directiva solo se preveía como transferencia internacional la cesión de datos a terceros países, el Reglamento amplía el sujeto destinatario a organizaciones internacionales, que son definidas en el artículo 4.26 de forma muy imprecisa[25]. Esta previsión puede llegar a ser problemática, ya que no se tiene en cuenta en la regulación el país donde esté ubicada la misma. En este sentido, no es lo mismo que la organización esté dentro del espacio EEE a que se sitúe fuera. No obstante, las características propias de estos sujetos de derecho internacional, con autonomía jurídica respecto de los países que la forman, hace necesario su referencia expresa en el Reglamento[26].

Por otro lado, otra novedad importante en el RGPD se refiere a que se permiten, como regla general, las transferencias internacionales no solo cuando el país tercero u organización internacional de que se trate ofrezca un nivel adecuado de protección (artículo 45), sino que se amplía a los supuestos en que el responsable y encargado de tratamiento ofrezcan garantías adecuadas (artículo 46). Es decir, este último supuesto pasa de ser una de las excepciones previstas en el artículo 26 de la

---

[24] Así lo pone de manifiesto PIÑAR MAÑAS, J. L., "Transferencias de datos personales a terceros países u organizaciones internacionales", *op. cit.,* pág. 428.

[25] "Organización internacional": una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

[26] PIÑAR MAÑAS, J. L., "Transferencias de datos personales a terceros países u organizaciones internacionales", *op. cit.,* pág. 439.

Directiva, a ser considerado un supuesto normal, permitido sin autorización, para que se realice una transferencia internacional de datos.

Por consiguiente, y siguiendo al profesor PIÑAR MAÑAS, será posible una transferencia internacional de datos a un tercer país u organización internacional cuando:

- Se base en una decisión de adecuación
- Se base en garantías adecuadas
- Se base en alguna de las excepciones previstas en el artículo 49 del RGPD[27]

Teniendo en cuenta lo anterior, es importante, en primer lugar, señalar quien puede emitir una decisión de adecuación. En este sentido, el artículo 45.1 señala que será la Comisión quien decida qué "tercer país, territorio, sector específico u organización internacional" de que se trate, garantizan un nivel adecuado para que la transferencia no requiera ninguna autorización específica. Para dictar esa decisión, que se hace mediante un acto de ejecución, la Comisión debe evaluar una serie de elementos del tercer país, territorio, sector específico u organización internacional (artículo 45.2 del RGPD)[28]. Llama la atención la posibilidad

[27] *Ibidem,* pág. 434.

[28] 2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados

de que la decisión afecte no solo a un tercer país, sino también a un territorio (de un tercer país, se entiende) o sector específico. Ya se había admitido la posibilidad de que la decisión de adecuación afectase, exclusivamente, a un determinado número de empresas en un país determinado[29], pero ahora se indica la posibilidad de que afecte a uno o varios territorios específicos, en el supuesto, según estimo, de que se trate de un estado compuesto o federal que reconozca cierta autonomía a los territorios que lo componen. En la misma línea, se puede reconocer un nivel de adecuación a uno o varios sectores específicos.

Como ya se ha indicado, otro supuesto normal de transferencia internacional de datos que no necesita autorización es que el responsable o encargado de tratamiento ofrezcan garantías adecuadas y "a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas (artículo 46.1, ***in fine***). Estas garantías adecuadas pueden prestarse, según lo dispuesto en el artículo 46.2 del RGPD, mediante:

a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
b) normas corporativas vinculantes;
c) cláusulas tipo de protección de datos adoptadas por la Comisión;
d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión;

---

en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

[29] En este sentido, el sistema de Puerto Seguro, hoy sustituido por el *Privacy Shield*, permite que se realicen transferencias internacionales con determinadas empresas estadounidenses adheridas al mismo. Como es sabido, la Sentencia del Tribunal de Justicia de la Unión Europea en el asunto Sentencia en el asunto C-362/14 *Maximillian Schrems/Data Protection Commissioner*, de 6 de octubre de 2015, invalidó el sistema de Puerto Seguro, t tuvo que ser sustituido, después de unos meses de incertidumbre, por la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de junio de 2016 por el conocido como sistema de "Escudo de Seguridad"

e) un código de conducta[30];
f) un mecanismo de certificación.

Mención especial merecen las normas corporativas vinculantes[31], pues son una de las principales novedades del RGPD. Se definen en el artículo 4.20 como: "las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta". Estas normas corporativas vinculantes o BCR's, han planteado algún problema en el pasado, pues se trata, en definitiva, de supuestos de autorregulación. No obstante, hay que señalar que el RGPD ha venido a aclarar, en gran medida, las dudas que planteaban, pues se realiza una regulación muy detallada y extensa en el artículo 47, donde se establecen los requisitos que tienen que cumplir y el contenido mínimo de las mismas[32]. Así, como requisitos, el artículo 47.1 señala que:

30 Sobre los códigos de conducta en el nuevo RGPD, véase DÍAZ-ROMERAL GÓMEZ, A., "Códigos de conducta en el Reglamento General de Protección de Datos" en PIÑAR MAÑAS, J. L. (Director), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, op. cit.,* págs. 389 a 411.

31 Sobre las normas corporativas vinculantes o BCR's, se deben tener en cuenta los documentos sobre la materia publicados por el Grupo de Trabajo del artículo 29, de entre los que cabe destacar, en mi opinión: WP212 *Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents*; y WP155 *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, entre los muchos trabajos publicados.*

32 PIÑAR MAÑAS, J. L., "Transferencias de datos personales a terceros países u organizaciones internacionales"*, op. cit.,* pág. 452, "Desde el punto de vista de las BCRs como fuente de obligaciones para los responsables y encargados el tema capital es el de su carácter vinculante en cuento declaración unilateral de voluntad. Las posibles dudas que podrían plantearse entre nosotros teniendo en cuenta el sistema del Código Civil hoy deben entenderse disipadas dado que las normas corporativas vinculantes, como tales, se recogen expresamente en una norma jurídica de directa aplicación como es un Reglamento de la Unión Europea. Una muestra más del alcance de la regulación de la protección de datos en nuestro ordenamiento."

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado, es decir, que tengan, como mínimo, esos elementos[33].

[33] El contenido mínimo de las normas corporativas vinculantes viene recogido en el artículo 47.2 del RGPD:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

Para terminar este epígrafe, debemos hacer una breve referencia a las excepciones para situaciones específicas recogidas en el artículo 49 del RGPD. Según este precepto: en ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los

---

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;
c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;
d) la transferencia sea necesaria por razones importantes de interés público;
e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;
f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;
g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

En alguno de estos supuestos, por consiguiente, no será necesaria una autorización de las autoridades de control para realizar la correspondiente transferencia internacional. Este elenco de excepciones debe considerarse como *numerus clausus*, aunque algunas de ellas están enunciadas en términos muy amplios[34].

[34] PIÑAR MAÑAS, J. L., "Transferencias de datos personales a terceros países u organizaciones internacionales", *op. cit.,* pág. 455.

5.- La protección de datos en el Reino Unido tras la salida de la Unión Europea. Escenarios hipotéticos

5.1.- El escenario más improbable. Abandono efectivo antes del 25 de mayo de 2018. Aplicación de la Directiva

Este parece el escenario más improbable, debido, fundamentalmente, a que parece que la salida va a ir precedida de un largo proceso negociador que en ningún caso parece que vaya a resolverse antes de que la aplicación del RGPD sea efectiva. De hecho, tras la activación del artículo 50 del TUE el pasado 29 de marzo, el Gobierno británico prevé que el abandono definitivo se produzca en marzo de 2019, es decir, una vez sea aplicable el RGPD también en Reino Unido. No obstante, hay que tener en cuenta la posibilidad de que las posiciones se enconen y Reino Unido decida una separación drástica, sin negociación previa. Escenario francamente improbable pues sería la versión más extrema del denominado ***hard Brexit***, pero a tener en cuenta, pues nada impide, por el momento, que se pueda materializar[35].

---

[35] Se debe mencionar que esta era una de las posibilidades por la que optaban algunos autores antes de la incorporación del artículo 50 al Tratado de la Unión Europea. Es decir, una salida drástica y sin autorización y apenas negociación con la Unión. Así lo describe, magníficamente, TATHAM, A. F., "'Don't Mention Divorce at the Wedding, Darling!': EU Accession and Withdrawal after Lisbon", en BIONDI, A., EECKHOUT, P., and RIPLEY, S., *EU Law after Lisbon*, Oxford Scholarship Online, 2012, "*Until the advent of the 2004 Constitutional Treaty, neither the original founding Treaties nor the succeeding treaties contained a provision allowing Member States to withdraw or secede—either in a negotiated or a unilateral manner—from the Union"*

"Nevertheless, those submissions generally reflected the three potential models for withdrawal mechanisms:140 (a) state primacy, where a Member State has an absolute, immediate and unilateral right to withdraw from a federation. This was essentially advocated by Dashwood and meant that the Member State had an unconditional right which did not require permission from EU institutions; (b) federal primacy, where a Member State is absolutely prohibited from withdrawing. Lamassoure did discuss the fact that in a federal141 restructuring (p.148) of the EU, the rule should be 'once a member, always a member' but regarded this and the confederal142 model as extremes. He therefore proposed a community option allowing withdrawal but 'subject to strict and deterrent conditions'; and (c) federal control, where a Member State retains its sovereign right to withdraw, subject to negotiations with and the approval of the remaining states in the federation, thereby emphasizing the process as a mutually negotiated activity. Badinter's proposal, given in a more detailed manner, firmly followed this option and was closer to what was actually drafted for Article I-60 of the 2004 Constitutional Treaty. Although it never entered into force, its contents were later reproduced in the Lisbon Treaty with only minor technical changes"

En este escenario, Reino Unido sería considerado a todos los efectos como un tercer país y, por consiguiente, las transferencias de datos a su territorio deberían ser consideradas transferencias internacionales. Pero, además, al no ser aplicable todavía el RGPD, habría que tener en cuenta la regulación recogida en la Directiva[36] y las correspondientes normas nacionales. En este sentido, la norma general es que solo se permiten transferencias internacionales previa decisión de adecuación, con las excepciones ya mencionadas más arriba. Hay que tener en cuenta que es improbable que esa decisión de adecuación se produjese antes del 25 de mayo de 2018, por lo que, seguramente, la Comisión esperaría a que el RGPD fuese aplicable. En este sentido, las transferencias de datos antes del 25 de mayo de 2018 deberían ampararse en alguna de las excepciones previstas en el artículo 26 de la Directiva, incluido, por tanto, las garantías suficientes ofrecidas por el responsable.

Por otro lado, cabe mencionar que de producirse esta separación unilateral, el Reino Unido tendría que adaptar su legislación interna para adaptarse al RGPD "a fin de asegurar que el nivel de protección de las personas físicas garantizado por el Reglamento no se vea menoscabado" (artículo 44). Y es que, las novedades introducidas por el Reglamento son importantes y de hondo calado, por lo que el Reino Unido debería adaptarse a las mismas si, en este escenario improbable, repito, aspirase a una decisión de adecuación por parte de la Comisión.

Otra cuestión distinta, ya de índole político, es que la Comisión quisiera "castigar" esa decisión de separación unilateral. En este sentido, no sería tan fácil conseguir esa decisión de adecuación y habría que acudir a otros sistemas previstos en el RGPD, en los términos señalados más arriba.

[36] La Directiva es aplicable, pese a su derogación, hasta el 25 de mayo de 2018, en los términos previstos en el artículo 94.1 del RGPD.

5.2.- Abandono efectivo después del 25 de mayo de 2018, pero sin negociación específica sobre protección de datos.

Con fecha 19 de junio de 2017, Michel Barnier, negociador principal de la UE, y David Davis, ministro para la Salida de la Unión Europea, inician la primera ronda de negociaciones del *Brexit*. Este acto de un día de duración se celebra en Bruselas.

A parte de tratar el tema de cómo se realizarán las siguientes negociaciones, esta primera reunión se centra en tres cuestiones esenciales: derechos de los ciudadanos; la liquidación financiera; y la frontera de Irlanda del Norte. No se incluye en la agenda, por el momento, un posible acuerdo sobre el derecho a la protección de datos, aunque no es en absoluto descartable.

Por tanto, es probable que el Reino Unido abandone la Unión después del 25 de mayo de 2018 y que los representantes de ambas partes no hayan negociado la futura relación entre ambos en materia de protección de datos. En este caso, el RGPD también habrá sido aplicado durante un plazo de tiempo determinado, en concreto hasta que se produzca la separación definitiva. Imaginemos que, como parece probable, la salida no se produce hasta la primavera de 2019. En este caso, el RGPD se habrá aplicado en Reino Unido durante casi un año, y posteriormente seguirá ejerciendo influencia, por inercia, en las normas posteriores que se puedan aprobar.

Esta parece ser la idea que tiene el Gobierno británico, es decir, en primer lugar, que el RGPD se aplique en su territorio una vez se llegue a la fecha prevista y, por otro lado, continuar con el espíritu de protección del derecho fundamental a la protección de datos que establece el RGPD y otras normas europeas. No va a haber, por tanto, según parece, una ruptura total del Reino Unido respecto a la protección de este derecho fundamental. Así lo ha manifestado, expresamente, la autoridad de control británica[37] (*Information Commissioner's Office* o

[37] Resulta necesario resaltar que la actual directora de la autoridad de control británica (ICO), Elizabeth Denham, es de nacionalidad canadiense y ha ocupado el cargo de *Privacy Commissioner for British Columbia* en Canada. Este hecho puede llevar al optimismo en cuanto a la postura que adoptará Reino Unido durante y después del *Brexit*, por la dimensión internacional de la persona que está al mando de la autoridad de control independiente.

ICO, por sus siglas en inglés) en su estrategia internacional para los años 2017-2011[38], aprobada en julio de 2017. De hecho, su intención es participar activamente en el Comité Europeo de Protección de Datos[39] mientras permanezca en la Unión y mantener relaciones con el resto de autoridades nacionales y europeas, en mayor beneficio de la protección del derecho fundamental.

Si esto es así, lo más probable es que una vez se produzca la salida del Reino Unido de la Unión, la Comisión dicte una decisión de adecuación del nivel de protección de datos para Reino Unido, de manera que se permitan las transferencias internacionales a su territorio en los términos establecidos en el artículo 45 del RGPD. No obstante, hasta que se dicte esa decisión de adecuación, los flujos de datos entre

---

[38] Según este documento, el *Brexit* es uno de los principales retos a los que se enfrenta Reino Unido en materia de protección de datos, y expresamente se indica que: *"As the UK prepares to leave the EU, the formal relationship between the ICO and EU data protection authorities will change. Our relationship with our EU partners will remain highly important, including with the European Data Protection Board (EDPB) which will operate from May 2018 and on which the ICO will remain active and engaged until the UK's exit. In overseeing the enforcement of the General Data Protection Regulation (GDPR) from 2018, and issuing guidance, the EDPB will be a highly influential global player in setting the direction for data protection and privacy standards.*

The strategy recognises that our direction on many of these challenges will often be driven by the outcome of the negotiations between the UK and the EU. Our priorities are designed to be compatible with a range of scenarios and enable the ICO to respond flexibly to different circumstances.

In 2017, the Secretary of State, Karen Bradley, and the UK Minister responsible for the digital economy, Matthew Hancock, made several statements to Parliament declaring the UK Government's commitment to comprehensively implementing GDPR, as planned, in 2018. The June 2017 Queen's Speech included a commitment to introduce a Data Protection Bill:

"To implement the General Data Protection Regulation and the new Directive which applies to law enforcement data processing, meeting our obligations while we remain an EU member state and helping to put the UK in the best position to maintain our ability to share data with other EU member states and internationally after we leave the EU."

Our strategy presumes that GDPR will also be assumed into UK law before exit to ensure there is continuity and certainty about UK law afterwards.

The ICO recognises the importance of the UK retaining a high standard of data protection and data protection as a fundamental right. Our strategy recognises the possible role of EU laws and the Council of Europe in this after Brexit, directly or indirectly.

[39] El Comité Europeo de Protección de Datos es el órgano que viene a sustituitr al Grupo de Trabajo del artículo 29 de la Directiva. Como es sabido, el Grupo de Trabajo del artículo 29 ha tenido un papel fundamental en la interpretación de la Directiva. Los documentos publicados han sido un referente en la materia y el representante del Reino Unido ha sido, tradicionalmente, muy activo. El RGPD viene a reforzar esa posición al atribuir el Comité muy relevantes funciones según lo previsto en el artículo 70

la Unión y Reino Unido deberán ampararse en alguna de las formulas previstas en el artículo 46 (garantías adecuadas), artículo 47 (BCR´s) o las excepciones del artículo 49, como ya se ha señalado en otro lugar.

5.3.- Abandono efectivo después del 25 de mayo de 2018, con negociación específica sobre protección de datos.

Otra posibilidad es que se incluya la materia de protección de datos en la agenda negociadora del *Brexit*. En este sentido, habrá que estar a lo que se establezca en esas negociaciones, en la que caben un amplio abanico de posibilidades. Por ejemplo, que se le ofrezca un status especial a Reino Unido en esta materia, con representación (como observador u otro rol) en el Comité Europeo de Protección de Datos, o que se acuerde el flujo libre de datos entre ambos, sin que sean considerados transferencia internacional, en una posición similar a la que tienen los países que forman parte del Espacio Económico Europeo (pero sin formar parte de él), con los que no sería necesario acudir a las herramientas establecidas para una transferencia internacional, como es sabido. Es lo que algunos autores han denominado el *The 'go it alone' model*[40].

5.4.- Incorporación al Espacio Económico Europeo una vez haya abandonado la Unión.

Esta quizás sea la postura más sencilla, pero tiene claros inconvenientes políticos para el Reino Unido, porque deberá explicar a la ciudadanía que pese a haber abandonado la Unión se mantienen muchas de las políticas procedentes de la Unión Europea. Además, con una posición mucho menos relevante para influir en la adopción de dichas políticas.

---

[40] MULLOCK, J., y SHOOTER, S "*Brexit: Data protection and cybersecurity law implications*", que se puede consultar en el siguiente enlace: https://www.twobirds.com/en/news/articles/2016/uk/brexit-data-protection-and-cyber-security-law-implications.

Sin embargo, en materia de protección de datos sería, quizás, lo más adecuado, teniendo en cuenta que el flujo de datos entre los miembros del EEE es libre y, por tanto, no se considera transferencia internacional según lo dispuesto en el RGPD

6.- En cualquiera de los escenarios, el Reino Unido debe tener en cuenta las previsiones del RGPD

No obstante los escenarios a los que antes me he referido, se ha de tener en cuenta que el ámbito de aplicación territorial del RGPD, recogido en el artículo 3, hace que en el Reino Unido no se pueda desdeñar la aplicación del RGPD

Así, se establece que el Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido[41] en la Unión cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

Es decir, que independientemente del lugar de establecimiento (incluso en terceros países) del responsable o encargado de tratamiento, el RGPD se aplica cuando se den algunos de estos supuestos. En definitiva, incluso en el peor de los escenarios, con una ruptura unilateral sin que se adapten las novedades del Reglamento a la legislación interna británica, este seguirá siendo aplicable en los supuestos señalados en el artículo 3. Cuestión distinta es que las decisiones de aplicación del RGPD puedan ser adecuadamente ejecutadas en territorio británico.

[41] Puede verse, en este sentido, RIPOL CARULLA, S., "Aplicación territorial del Reglamento", en en PIÑAR MAÑAS, J. L. (Director), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, op. cit.,* págs. 77 a 95.

7.- Conclusiones

El abandono de la Unión Europea por parte del Reino Unido va a tener importantes consecuencias en materia de protección de datos. Y es que, pasará a ser, salvo su incorporación al EEE, un tercer país a efectos de aplicación del RGPD, por lo que habrán de tenerse en cuenta las herramientas previstas para las transferencias internacionales, con todas las dificultades y costes que ello genera para las empresas.

Parece, no obstante, que el Reino Unido hará todo lo posible por mantener el espíritu de protección adecuada del derecho fundamental a la protección de datos. Y en este sentido, según ha manifestado el ICO y el propio Gobierno británico, su intención es trasladar al ordenamiento interno los principios recogidos en el RGPD, con todas las novedades que conlleva. Ello supondrá que, de no incorporarse al EEE, obtendrá, casi con total seguridad, el reconocimiento, por parte de la Comisión, de una decisión de adecuación.

En cualquier caso, y hasta que esa decisión de adecuación sea efectiva, las transferencias de datos de empresas radicadas en la Unión hacia el Reino Unido, que no serán pocas pues los lazos económicos y sociales son muy estrechos, habrán de ampararse en cualquiera de los supuestos recogidos en el RGPD, es decir, desde las garantías adecuadas (las BCR's parecen las más idóneas), hasta las excepciones previstas en el artículo 49.

Más allá, por tanto, de una decisión que pone en entredicho el proyecto europeo común, se observa como la salida del Reino Unido de la Unión Europea implica importantes consecuencias de orden práctico que deberán ser salvadas por las empresas y entidades públicas correspondientes.

8.- Bibliografía

CRAIG, P., *"Brexit: A Drama in Six Acts", European law review,* núm. 4, 2016

DÍAZ-ROMERAL GÓMEZ, A., "Códigos de conducta en el Reglamento General de Protección de Datos" en PIÑAR MAÑAS, J. L. (Director), y ÁLVAREZ CARO M., y RECIO GAYO, M., (Coordinadores), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016

GUASCH PORRAS, V., *Las transferencias internacionales de datos en la normativa española y comunitaria*, edición conjunta de la Agencia Española de Protección de Datos y la Agencia Estatal Boletín Oficial del Estado, Madrid, 2014

JAMES, S., y QUAGLIA, L., "*The political economy of finance in the UK and Brexit*", en *The Political Economy of Brexit and the UK's National Business Model*, SPERI Paper No. 41, 2017

MARTÍN DELGADO, I., "Brexit means Brexit… o no. Especulaciones, conjeturas y algunas consideraciones jurídicas al propósito de la decisión del Reino Unido de retirarse de la Unión Europea en el contexto del artículo 50 del TUE", *El Cronista del Estado Social y Democrático de Derecho*, núm. 64.

MULLOCK, J., y SHOOTER, S "*Brexit: Data protection and cybersecurity law implications*", https://www.twobirds.com

PIÑAR MAÑAS, J.L., "Transferencias de datos personales a terceros países u organizaciones internacionales" en PIÑAR MAÑAS, J. L. (Director), y ÁLVAREZ CARO M., y RECIO GAYO, M., (Coordinadores), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016

REMOLINA, N., *Recolección internacional de datos personales: un reto del mundo post-internet*, edición conjunta de la Agencia Española de Protección de Datos y la Agencia Estatal Boletín Oficial del Estado, Madrid, 2014

RIPOL CARULLA, S., "Aplicación territorial del Reglamento" en PIÑAR MAÑAS, J. L. (Director), y ÁLVAREZ CARO M., y RECIO GAYO, M., (Coordinadores), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016

SARMIENTO, D., "Y después del Brexit… ¿Qué?", *El Cronista del Estado Social y Democrático de Derecho*, núm. 64

TATHAM, A. F., "'Don't Mention Divorce at the Wedding, Darling!': EU Accession and Withdrawal after Lisbon", en BIONDI, A., EECKHOUT, P., and RIPLEY, S., *EU Law after Lisbon*, Oxford Scholarship Online, 2012

TORREGROSA VÁZQUEZ, J., "Revisión de otros actos jurídicos de la Unión en materia de Protección de Datos, entrada en vigor y aplicación del Reglamento", en PIÑAR MAÑAS, J. L. (Director), y ÁLVAREZ CARO M., y RECIO GAYO, M., (Coordinadores), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016

WELFENS, P. J. J., "Cameron's information disaster in the referendum of 2016: an exit from Brexit?", *International Economics and Economic Policy*, octobre, 2016