UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO

RAPHAELA JÉSSICA REINALDO CORTEZ

PROVA DIGITAL NO PROCESSO PENAL BRASILEIRO: O USO DE DADOS DE GEOLOCALIZAÇÃO NA SEGURANÇA PÚBLICA E NA INVESTIGAÇÃO CRIMINAL

NATAL/RN
2023

RAPHAELA JÉSSICA REINALDO CORTEZ

PROVA DIGITAL NO PROCESSO PENAL BRASILEIRO: O USO DE DADOS DE GEOLOCALIZAÇÃO NA SEGURANÇA PÚBLICA E NA INVESTIGAÇÃO CRIMINAL

Dissertação apresentada ao programa de Pós-graduação em Direito, da Universidade Federal do Rio Grande do Norte, como requisito parcial à obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Walter Nunes da Silva Júnior

NATAL/RN

2023

Universidade Federal do Rio Grande do Norte - UFRN
Sistema de Bibliotecas - SISBI
Catalogação de Publicação na Fonte. UFRN - Biblioteca Setorial do Centro Ciências Sociais Aplicadas - CCSA

Cortez, Raphaela Jéssica Reinaldo.
Prova digital no processo penal brasileiro: o uso de dados de geolocalização na segurança pública e na investigação criminal / Raphaela Jéssica Reinaldo Cortez. - Natal, 2023.
104f.: il.

Dissertação (Mestrado em Direito) - Universidade Federal do Rio Grande do Norte, Centro de Ciências Sociais Aplicadas, Programa de Pós-Graduação em Direito. Natal, RN, 2023.
Orientador: Prof. Dr. Walter Nunes da Silva Júnior.

1. Processo penal - Dissertação. 2. Prova digital - Dissertação. 3. Direitos fundamentais - Dissertação. 4. Dados de localização - Dissertação. 5. Direito à intimidade - Dissertação. 6. Direito à privacidade - Dissertação. I. Silva Júnior, Walter Nunes da. II. Título.

RN/UF/Biblioteca CCSA CDU 343.14:342.7

Elaborado por Eliane Leal Duarte - CRB-15/355

RAPHAELA JÉSSICA REINALDO CORTEZ

PROVA DIGITAL NO PROCESSO PENAL: O USO DE DADOS DE GEOLOCALIZAÇÃO NA SEGURANÇA PÚBLICA E NA INVESTIGAÇÃO CRIMINAL

Dissertação apresentada ao programa de Pós-graduação em Direito da Universidade Federal do Rio Grande do Norte, como requisito parcial à obtenção do título de Mestre em Direito.

Aprovada em: _____/_____/_____

BANCA EXAMINADORA

_____

Prof. Dr. Walter Nunes da Silva Júnior

Orientador

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

_____

Profa. Dra. Yara Maria Pereira Gurgel

Membro interno

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

_____

Prof. Dr. Gustavo Henrique Righi Ivahy Badaró

Membro externo

UNIVERSIDADE DE SÃO PAULO

Ao meu marido, Rodolpho Luiz Araújo Cortez, e à nossa filha, Clara, – ainda com dezenove semanas – que me ensinaram, com muita paciência e amor, que não há limites para realizar um sonho.

AGRADECIMENTOS

Agradeço a Deus pelas oportunidades e pela possibilidade de concluir este trabalho, o qual dedico especialmente:

Ao meu orientador de dissertação de Mestrado, professor Walter Nunes da Silva Júnior, a quem devo o amor pelo direito processual penal, a busca pelo rigor técnico e o espírito de defesa dos direitos fundamentais. À professora Yara Maria Pereira Gurgel pelas valiosas contribuições ao longo dos dois anos de mestrado e ao professor Gustavo Henrique Righi Ivahy Badaró por, além de ser fonte de inspiração na área acadêmica e profissional, aceitar participar da avaliação deste trabalho e contribuir de forma fundamental.

À minha família, pela paciência e apoio, indispensáveis para que eu pudesse me dedicar a este trabalho, em especial à minha mãe, Rita das Mercês Reinaldo, e ao meu sobrinho, Guilherme de Negreiros Diógenes Reinaldo.

Aos amigos e companheiros dessa caminhada acadêmica, Francisco Sidney de Castro Ribeiro, Ívinna Ellionay Alves dos Santos, Lorenna Medeiros Toscano de Brito e Marcela Cardoso Linhares Oliveira, por dividirem as angústias e vitórias ao longo desses dois anos.

Por fim, à todos aqueles que contribuíram, direta ou indiretamente, para a realização desta dissertação, o meu sincero agradecimento.

Ao futuro ou ao passado, a um tempo em que o pensamento seja livre, em que os homens sejam diferentes uns dos outros, em que não vivam sós – a um tempo em que a verdade exista e em que o que for feito não possa ser desfeito.

George Orwell.

RESUMO

A presente dissertação busca analisar o impacto do desenvolvimento tecnológico na área da segurança pública e na investigação criminal, especialmente no que se refere à produção e utilização de provas digitais relacionadas aos dados de localização, isso porque o avanço da tecnologia contida em dispositivos eletrônicos impôs novos e expressivos desafios ao direito probatório no processo penal. Atualmente, a ausência de regulamentação específica sobre essa nova fonte de prova ou a aplicação de legislações ultrapassadas possibilitam a violação do direito à intimidade e à privacidade do investigado. Considerando essa realidade, o estudo tem como objetivo principal demonstrar, com base da teoria do garantismo penal, a viabilidade de utilização de recursos tecnológicos como fonte de prova para o processo penal, respeitando a proteção de direitos e garantias fundamentais dos cidadãos, além de contribuir para uma maior eficiência na segurança pública e nas investigações criminais. Para tanto utilizou-se do método dedutivo, através de revisão de doutrina jurídica nacional e estrangeira, sistematização de decisões judiciais proferidas nos últimos anos sobre a utilização de provas digitais no processo penal e análise dos dados sobre a ineficiência das investigações criminais quanto à identificação de possíveis autores de crimes no âmbito do estado do Rio Grande do Norte. Após a análise dos pressupostos teóricos mencionados, percebe-se que a ordem jurídica brasileira carece de normativa específica sobre o conteúdo de dados de localização como fonte de prova para o processo penal. Sugere-se, ao final, a adoção de disciplina jurídica desenvolvida com base na Convenção de Budapeste em conjunto com a normativa da ABNT NBR ISO/IEC 27037:2012 e o Anteprojeto da LGPD Penal.

Palavras-chave: dados de localização; prova digital; processo penal; direitos fundamentais; direito à intimidade e à privacidade.

ABSTRACT

This study aims to analyze the impact of technological development in the area of public security and criminal investigation, especially with regard to the production and use of digital evidence related to location data, because the advancement of technology contained in electronic devices has imposed new and significant challenges to the law of evidence in criminal proceedings. Currently, the lack of specific regulation on this new source of evidence or the application of outdated legislation allows the violation of the right to privacy and intimacy of the person under investigation. Considering this fact, the purpose of this study is to demonstrate, based on the theory of penal garantism, the viability of using technological resources as a source of evidence in the criminal process, respecting the protection of the fundamental rights of citizens, as well as contributing to a more efficient public security and criminal investigations. To achieve this, the deductive method was used, through the review of national and foreign legal doctrine, systematization of court decisions issued in the last years on the use of digital evidence in criminal proceedings and analysis of data on the inefficiency of criminal investigations for the identification of possible authors of crimes in the state of Rio Grande do Norte. After the analysis of the theoretical assumptions mentioned, it can be seen that the Brazilian legal system has a lack of specific normative on the content of location data as a source of evidence for the criminal process, suggesting, in the end, the adoption of legal discipline developed based on the Budapest Convention in conjunction with the ABNT NBR ISO/IEC 27037:2012 normative and the Draft of the Criminal LGPD.

Keywords: location data; digital evidence; criminal procedure; fundamental rights; right to intimacy and privacy.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
ADI	Ação Direta de Inconstitucionalidade
ADPF	Arguição de Descumprimento de Preceito Fundamental
CADH	Convenção Americana de Direitos Humanos
CDC	Código de Defesa do Consumidor
CDPC	Comitê Europeu para os Problemas Criminais
CF	Constituição da República Federativa do Brasil
CNJ	Conselho Nacional de Justiça
CNPCP	Conselho Nacional de Política Criminal e Penitenciária
Corte IDH	Corte Europeia de Direitos Humanos
CPC	Código de Processo Civil
CPP	Código de Processo Penal
DEPEN	Departamento Penitenciário Nacional
ERB	Estações Rádio Base
EUA	Estados Unidos da América
GPS	Sistema de posicionamento global
IEC	Comissão Eletrotécnica Internacional
IP	Protocolo de internet
IRIS	Instituto de Referência em Internet e Sociedade
ISSO	Organização Internacional de Padronização
JFRN	Justiça Federal do Rio Grande do Norte
LBS	*Location-based services*
LGPD	Lei Geral de Proteção de Dados
LGPD Penal	Lei de Proteção de Dados para a segurança pública e investigação criminal
MJSP	Ministério da Justiça e Segurança Pública
OBVIO	Observatório de Violência do Rio Grande do Norte
OIT	Organização Internacional do Trabalho
ONU	Organização das Nações Unidas
PC-CY	Comitê de Especialistas sobre a Criminalidade no Ciberespaço
POP	Procedimento Operacional Padrão
RENAPE	Registro Nacional de Pessoas Naturais
RFID	Identificação de radiofrequência

RMS Recurso Ordinário em Mandado de Segurança

SENASP Secretaria Nacional de Segurança Pública

SINESP-PPE Sistema de Informações de Segurança Pública, Prisionais e sobre Drogas – Procedimentos Policias Eletrônicos

STF Supremo Tribunal Federal

STJ Superior Tribunal de Justiça

SWGDE *Standard Working Group on Digital Evidence*

UFRN Universidade Federal do Rio Grande do Norte

WI-FI *Wireless fidelity*

SUMÁRIO

1 INTRODUÇÃO

A área de segurança pública e investigação criminal tem vivenciado mudanças significativas ao longo dos últimos anos e mesmo possuindo finalidades distintas, a atividade preventiva e pós delitiva, respectivamente, vêm reconhecendo a urgência em se adaptarem às novas tecnologias. A quantidade de dados obtidos através das mais diversas ações do ser humano tem crescido de forma célere e exponencial, o que tem gerado discussões sobre a proteção, tratamento e segurança dessas informações, especialmente no âmbito criminal.

Atualmente, essa produção massiva de dados digitais se apresenta como o instrumento de maior valor para a sociedade e, portanto, demanda um maior controle sobre a sua utilização. Nesse sentido, para que sejam evitados os perigos de um poder ilimitado sobre o uso dos dados pessoais coletados, é importante, em um primeiro momento, desassociar o poder informacional do poder de persecução penal, isso porque se for permitida a reunião dessas duas formas de controle, sem qualquer forma de limitação, maior será a probabilidade da ocorrência de abusos na seara processual.

Nesse ponto, dois interesses legítimos entram em conflito: o interesse do investigado em resguardar a sua privacidade diante da vigilância estatal e o interesse do estado em solucionar os delitos e proporcionar segurança à sociedade. Dessa maneira, despontam os seguintes questionamentos: quais os limites para flexibilização do direito à intimidade e à privacidade no âmbito da segurança pública e das investigações criminais? Os novos recursos tecnológicos podem servir como fonte de prova para o processo penal? Como garantir a integridade da cadeia de custódia e a proteção aos dados pessoais coletados? A utilização do instrumento específico de geolocalização pode auxiliar na apuração de ilícitos visando uma maior eficiência quanto à identificação dos responsáveis?

Embora seja possível encontrar inúmeros estudos sobre a violação de garantias constitucionais que envolvem o tratamento dos dados digitais, o seu potencial para o desenvolvimento da segurança pública e de uma investigação criminal eficiente é inegável. Nesse ínterim, o projeto de pesquisa *Criminalidade violenta, justiça criminal e diretrizes para política de segurança pública do estado do Rio Grande do Norte*, através da elaboração do capítulo sobre *Os inquéritos policiais relativos aos crimes violentos letais intencionais no estado do Rio Grande do Norte e o dilema da ausência de identificação de autoria*, revelou que dos 223 (duzentos e vinte três) inquéritos policiais arquivados, 129 (cento e vinte e nove), no período de 2016 a 2020, foram motivados pela ausência de identificação de autoria (MEDEIROS *et al*., 2022, p. 56).

O objetivo do projeto de pesquisa supracitado concentra-se na investigação das causas dos altos índices de violência no estado do Rio Grande do Norte e na propositura de soluções criativas ao governo do Estado. Uma das investigações do projeto é voltada à análise da taxa de resolutividade de inquéritos policiais e o aprimoramento da atividade investigatória, o que se conecta diretamente com a presente dissertação, uma vez que pretende analisar se o avanço tecnológico na seara de produção de provas poderá auxiliar na busca por uma maior eficiência nas investigações iniciadas através de inquéritos policiais, sobretudo no estado do Rio Grande do Norte.

É importante ressaltar que o projeto mencionado está em consonância com a Agenda 2030 elaborada pela Assembleia Geral da Organização das Nações Unidas (ONU), ao qual engloba um compromisso firmado pelo Brasil e mais 192 (cento e noventa e dois) países membros visando a efetivação dos direitos humanos e a promoção do desenvolvimento sustentável através de 17 (dezessete) objetivos a serem alcançados durante o período de 15 (quinze) anos (2016 a 2030). O projeto enquadra-se, especificamente, no objetivo de desenvolvimento sustentável nº 16, que visa promover sociedades pacíficas e inclusivas para o desenvolvimento sustentável, proporcionar o acesso à justiça para todos e construir instituições eficazes, responsáveis e inclusivas em todos os níveis.

De forma gradual, percebe-se que o volume e a complexidade de informações obtidas através de fontes digitais têm exigido uma nova forma de aplicação da justiça criminal, provocando a discussão sobre a existência de uma regulamentação eficiente que seja capaz de, ao mesmo tempo, garantir a proteção de direitos fundamentais no âmbito do devido processo penal e obstar a ocorrência dos efeitos relacionados à manipulação abusiva dos dados digitais coletados. Nesse sentido, não se trata somente de proteger a privacidade dos dados, mas sim de proteger o indivíduo de uma coleta de dados desproporcional, sem qualquer regulamentação ou critérios que possam direcionar a atuação estatal.

A proteção à intimidade e à privacidade e a limitação do poder estatal sempre foram matérias apreciadas ao longo do tempo. O direito de estar só ou de controlar a sua exposição podem ser identificados desde os primórdios da Idade Antiga, em que foi possível identificar a reserva de assuntos religiosos ou políticos apenas aos membros de determinada família, ou até mesmo no direito à propriedade fortalecido ao longo da Idade Média, com o objetivo de possuir um espaço privado sem acesso do poder público.

Ocorre que, com as novas tecnologias, tem-se os novos perigos, como a possibilidade de um poder informacional desmedido do Estado e o desenvolvimento de consequentes ilações com base no comportamento público de alguém, cujo atos não estavam sendo observados

anteriormente. Assim, é necessário ter em mente de que se a sabedoria é poder, não é possível haver um poder ilimitado, tem que existir determinados instrumentos de proteção contra o uso irrazoável e desproporcional dos dados pessoais coletados, mesmo que seja em prol da segurança pública.

A acessibilidade à internet ou mesmo a necessidade de fornecimento de dados pessoais para obtenção de serviços básicos coloca o indivíduo em posição de desvantagem em relação ao poder estatal, visto que já não se trata de fornecimento optativo, mas muitas vezes obrigatório. Acontece que não é o poder público o principal detentor dessas informações, mas o poder privado que coleta e armazena os dados pessoais para, por exemplo, melhorar a prestação dos serviços que é oferecido e fomentar um capitalismo informacional. A partir desse fornecimento voluntário de dados, é que o Estado procura se tornar o detentor dessa informação em prol de um bem maior, como é o caso da segurança pública ou de investigações no âmbito criminal.

De fato, a discussão sobre a privacidade e o acesso de dados digitais encontra controvérsias não só no ambiente doméstico, mas também no âmbito internacional. Apesar de ser uma matéria discutida há alguns anos por diversos juristas e especialistas da área, a verdade é que a elaboração e aplicabilidade de normas voltadas à proteção de dados é recente no âmbito nacional, prova disso foi a publicação da Emenda Constitucional nº 115, no dia 10 de fevereiro de 2022, que incluiu o direito à proteção dos dados pessoais, inclusive nos meios digitais, no rol dos direitos e garantias fundamentais previstos no artigo 5º da Constituição Federal de 1988.

Apesar da recente previsão constitucional, o rápido avanço da tecnologia em detrimento da morosidade legislativa, já havia possibilitado a utilização de novos meios de obtenção de provas no âmbito criminal, muitos dos quais ainda padecem de questões polêmicas no âmbito jurídico e acadêmico, como é o caso do reconhecimento facial, banco de dados de DNA (ácido desoxirribonucleico) ou da coleta de dados gerais ou específicos, como os dados de geolocalização, retirados do dispositivo móvel de qualquer indivíduo.

Os dados de geolocalização são obtidos através de uma triangulação do sinal de internet do celular com Estações Rádio Base (ERB) ou de aplicativos existentes nos aparelhos que permitem que a autoridade pública consiga acessar os locais onde determinada pessoa se encontrava e, ainda pode permitir o acompanhamento em tempo real do indivíduo. Além dessas possibilidades, também é possível a utilização da tecnologia de *geofencing*, capaz de estabelecer um mapeamento de presença digital em um determinado perímetro geográfico, a partir do uso de sistema de posicionamento global (GPS), identificação de radiofrequência (RFID) ou sinais de *wireless fidelity* (Wi-Fi), por exemplo.

Por esse motivo, em um momento em que a velocidade da revolução tecnológica dos meios digitais ultrapassa de forma vertiginosa a regulamentação necessária ao seu uso, o objetivo geral deste trabalho é, através da teoria do garantismo penal, analisar a viabilidade da utilização de recursos tecnológicos como fonte de prova para o processo penal para que se tenha mais eficiência nas investigações desenvolvidas através de inquéritos policiais.

Para tanto, buscará em seu primeiro capítulo verificar quais são as garantias constitucionais extensíveis ao tratamento de dados digitais no âmbito da segurança pública e na investigação criminal, pontuando no primeiro tópico a dicotomia entre o direito à intimidade e à privacidade e o dever de proteção (eficiente) do poder estatal em prevenir e solucionar transgressões cometidas em território nacional. O segundo tópico, versará sobre os critérios necessários para o tratamento, armazenamento e segurança dos dados coletados no setor de segurança pública e investigação criminal.

No segundo capítulo, pretenderá delimitar o contexto em que a prova digital surgiu, definir seu conceito, natureza jurídica e as suas características, como forma de diferenciá-la das demais provas tradicionais existentes no processo penal. No segundo tópico deste capítulo, serão abordados os meios de obtenção e produção da prova digital, bem como o seu tratamento no campo da cadeia de custódia e de que forma será possível garantir a proteção de dados pessoais, tecendo, ao longo do terceiro item, breves comentários sobre o anteprojeto da lei geral de proteção de dados para segurança pública e persecução penal, com o objetivo de avaliar se a referida legislação está acompanhando o desenvolvimento fugaz das novas tecnologias.

Por fim, com a fundamentação consolidada nos capítulos anteriores, o terceiro capítulo tratará especificamente do uso de dados de geolocalização, contextualizando a sua origem e utilização ao longo da história. O primeiro tópico será responsável por delimitar os aspectos conceituais, as suas especificidades no âmbito das provas digitais e a sua inserção no Processo Penal. Já no segundo item serão apresentados os limites constitucionais que devem ser observados na utilização e obtenção de dados digitais através do instrumento de geolocalização, bem como a existência de normativas internacionais que possam auxiliar na delimitação no tratamento dos dados coletados. O último tópico apresenta, a partir dos estudos da literatura nacional, internacional e casos práticos, parâmetros propositivos à elaboração de uma regulamentação sobre a utilização de dados de geolocalização no setor de segurança pública e persecução penal.

Para atingir os objetivos delineados, a presente pesquisa utilizou-se do método dedutivo, buscando, em um primeiro momento, a revisão de doutrina jurídica especializada no âmbito nacional e internacional, uma vez que será necessário estabelecer parâmetros para a

conceituação das terminologias utilizadas, além de demarcar o referencial teórico a ser utilizado para o embasamento da pesquisa. Posteriormente, será realizada uma sistematização crítica de decisões judiciais proferidas nos últimos anos sobre a utilização de provas digitais no processo penal, visando compreender como o poder judiciário está se posicionando na aplicação dessa matéria em casos concretos. No entanto, considerando a precariedade de decisões no âmbito no estado do Rio Grande do Norte, será feito o levantamento de decisões já proferidas em âmbito nacional para uma melhor compreensão da temática.

Será analisado o levantamento de dados sobre a ineficiência das investigações quanto à identificação de possíveis autores de crimes realizados pelos participantes do projeto de pesquisa *Criminalidade violenta, justiça criminal e diretrizes para política de segurança pública do estado do Rio Grande do Norte*, buscando, ao final, identificar possíveis dificuldades encontradas na conclusão dessas investigações para que se possa propor critérios necessários para uma adequada disciplina jurídica, sobretudo do conteúdo de geolocalização como fonte de prova para o processo penal, a fim de que se tenha mais eficiência no desenvolvimento de inquéritos policiais.

Espera-se chegar à conclusão de que compete a todos os órgãos estatais e jurisdicionais competentes o dever de proteger os dados pessoais coletados através de investigações criminais, para que se possa viabilizar a correta utilização de recursos tecnológicos para otimização do desenvolvimento de inquérito policiais. Dessa forma, todos os sujeitos que possuírem acesso a esses dados serão considerados verdadeiros guardiões de informações pessoais sensíveis, sob pena de ser responsabilizado civil e criminalmente pelo seu descumprimento. Assim, o avanço tecnológico no âmbito do direito criminal poderá significar, especialmente, a diminuição do número de inquéritos policiais arquivados em virtude da ausência de identificação de possíveis autores.

Para fundamentar o resultado esperado, serão utilizadas lições doutrinárias, tanto de juristas nacionais como estrangeiros, dispositivos da Constituição Federal de 1988 e de normativas internacionais, jurisprudência dos Tribunais domésticos no que tange a aplicação na normativa existente sobre provas digitais no processo penal, bem como será incluída como base as pesquisas desenvolvidas no âmbito do projeto de pesquisa *Criminalidade violenta, justiça criminal e diretrizes para política de segurança pública do estado do Rio Grande do Norte*, vinculado à Universidade Federal do Rio Grande do Norte (UFRN).

2 DIREITOS CONSTITUCIONAIS FUNDAMENTAIS E O TRATAMENTO DE DADOS NA SEGURANÇA PÚBLICA E NA INVESTIGAÇÃO CRIMINAL

Um dos eixos para o desenvolvimento da ciência criminal pode ser encontrado nas modificações naturais que a vida em sociedade impõe, mas isso não significa dizer que o aperfeiçoamento dessa ciência ao longo dos anos nos levou a um procedimento atual infalível. Certamente, foi possível se distanciar de um período marcado por selvageria e barbáries, fomentados pelo "desejo incontrolável de dominação do homem pelo homem" (NUCCI, 2016, p. 16), e vislumbrar uma época em que já era possível discutir direitos que protegessem o bem mais precioso do ser humano: a vida.

No entanto, a verdade é que, enquanto a sociedade vem sendo naturalmente constituída em busca de progresso e da realização dos anseios no meio social, ela também demonstra as incoerências que poderiam permear a vida do homem em sociedade, isso porque, por mais contraditório que pareça, ao passo que ela é capaz de conferir segurança e prevenir crimes, é também apta a gerar insegurança e produzir criminalidade, sendo o crime inerente à vida em sociedade (SILVA JÚNIOR, p. 38, 2022).

De fato, ao longo dos anos, não houve sinais de conformismo da população – principalmente a parte mais vulnerável – diante das sanções físicas aplicada aos infratores, por isso, vários documentos foram elaborados, na tentativa de solucionar o problema da criminalidade e, ao mesmo tempo, conter os abusos do poder ilimitado dos soberanos e governantes. A Magna Carta (*Magna Charta*), de 1215, assinada pelo rei João Sem Terra, foi um dos primeiros documentos a prever direitos essenciais à liberdade humana, seguidos da Petição de Direitos (*Peticion of Rights)*, de 1628, o Ato de *Habeas Corpus* (*habeas Corpus* Act), de 1679 e a Declaração de Direitos (*Bill of Rights*), de 1689, os quais foram documentos que reconheceram direitos e liberdades aos cidadão ingleses, resultando em uma maior limitação ao poder monárquico e afirmação do parlamento perante a Coroa Inglesa (SARLET *et al*., 2015, p. 320).

Embora tais documentos tenham sua importância na história, especialmente para Inglaterra, foi somente com a Declaração de Direitos do Povo da Virgínia, de 1776, e a Declaração dos Direitos do Homem e do Cidadão, de 1789, que foram consagrados os primeiros direitos reconhecidos como fundamentais e que vieram contribuir para a estruturação da Declaração Universal dos Direitos Humanos, de 1948, aprovado pela Assembleia Geral das Nações Unidas (NUCCI, 2016, p. 18-20).

Após esse breve histórico sobre o tratamento de direitos, é importante concentrar-se na história do direito constitucional brasileiro, isso porque, seja em regimes democráticos ou ditatoriais, sempre foi possível encontrar a previsão de direitos fundamentais, prova disso foi a previsão sobre direitos civis e políticos dos cidadãos brasileiros na Constituição Imperial de 1824 (GROFF, 2008). Apesar do constituinte inserir no último artigo da Constituição de 1824 (art. 179), a previsão sobre a inviolabilidade dos direitos à liberdade, à segurança individual e à propriedade, tal fato representou o compromisso de garantir à nação brasileira, um generoso rol sobre direitos fundamentais, indo além da previsão disposta no projeto de Constituição apresentado inicialmente (SILVA JÚNIOR, 2022, p. 147).

Silva Júnior (2022, p. 147) ressalta, ainda, que dos trinta e cinco incisos inseridos na Constituição Imperial, quinze itens tratavam sobre garantias criminais, sendo trezes deles relacionados às questões processuais. Dentre eles, o inciso VII, o qual assegurava que "todo o cidadão tem em sua casa um asylo inviolável. De noite não se poderá entrar nella, senão por seu consentimento, ou para defender de incêndio, ou inundação; e de dia só será franqueada a sua entrada nos caos, e pela mandeira, que a Lei determinar". Apesar dessa previsão tratar sobre a inviolabilidade de domicílio, nota-se a intenção natural do legislador em resguardar a privacidade e a intimidade de qualquer indivíduo diante de possíveis arbitrariedades do estado, tema este que será melhor abordado no segundo tópico deste capítulo.

Em seguida, a Constituição de 1891, marcada pelo período republicano, manteve os direitos fundamentais assegurados aos brasileiros, reafirmando o princípio da inviolabilidade do domicílio, previsto no art. 73, § 11, além de ampliar o rol de garantias e direitos expressos na Constituição, incluindo, pela primeira vez, o direito ao sigilo da correspondência (art. 73, §18), o que reforça a intenção do constituinte em preservar o direito à intimidade do ser humano.

A Constituição de 1934 zelou pela manutenção desses direitos, diferentemente da Constituição de 1937, que foi marcada pelo Golpe de Estado e por características autoritárias e policialesca. Os direitos fundamentais declarados nessa constituição demonstram, nas palavras de Silva Júnior (2022, p. 154) "evidente retrocesso no respeito ao patrimônio histórico dos direitos do homem, arduamente conquistado ao longo dos tempos senão com lutas renhidas no universo das ideias e nos campos de batalha".

No estudo elaborado sobre *A busca e apreensão sob a ótica da redação originária do Código de Processo Penal de 1941*, desenvolvido no âmbito do projeto de pesquisa *Direito processual em movimento: ótica constitucional do processo criminal* vinculado à Universidade Federal do Rio Grande do Norte, foi possível analisar a limitação sofrida pelo direito constitucional à inviolabilidade do domicílio durante essa época. Extrai-se do texto que a

supressão da distinção da entrada ao domicílio durante o período da noite e do dia, prevista nas redações constitucionais anteriores, deixaram a cargo de leis ordinárias o tratamento sobre as hipóteses autorizadoras do ingresso, mesmo sem o consentimento do titular, o que deu margem à diversas arbitrariedades cometidas por agentes estatais em detrimento de direitos fundamentais anteriormente protegidos, representando um notório retrocesso na declaração dos direitos fundamentais (CORTEZ, 2023).

O direito à intimidade, como consequência lógica dos abusos cometidos, também foi cerceado. A Constituição de 1937, em seu art. 122, garantiu a inviolabilidade do domicílio e de correspondência, mas pôs a salvo as exceções previstas em lei, isto é, deixou a critério do legislador relacionar situações em que poderiam ocorrer a violação de correspondências, em nítido descompasso com a preservação de direitos fundamentais, já que se estava vivenciando um regime ditatorial, sem a existência de um poder legislativo independente.

O início desse regime se deu com a mobilização armada em busca de poder, em que foi deflagrado o golpe de Estado de 1930, levando ao início a Era Vargas[1]. A titularidade do poder governamental pelo Presidente Vargas, dividida em três momentos principais: o Governo Provisório, de 1930 a 1934, o Governo Constitucional, de 1934 a 1937 e o, tão conhecido, Estado Novo, marcado pela Constituição de 1937 até o ano de 1945, foi caracterizada por um momento de privilégio político, econômico e social concentrada nas mãos da elite brasileira.

Portanto, a inserção do direito à inviolabilidade previsto na Constituição de 1937, durante o Estado Novo, possuiu reflexos da concentração de poder nas mãos de um único representante, o Presidente da República, isso porque nesse período o Poder Judiciário e o Poder Legislativo estavam praticamente subordinados ao chefe do poder Executivo, já que cabia ao Presidente da República nomear o Presidente do Supremo Tribunal Federal, além de deter amplos poderes legislativos através da utilização de decreto-lei. Prova maior dessa ingerência executiva no âmbito legislativo foi a própria edição dos Códigos Penal e Processual Penal que foram inseridos através dos Decretos-Leis 2.848, de 7 de dezembro de 1940 e 3.689, de 3 de outubro de 1941, sem qualquer análise legislativa pelo Congresso Nacional (SILVA JÚNIOR, 2021, p. 111).

Acontece que, especialmente após a Segunda Guerra Mundial (1939-1945), foi possível reacender a discussão sobre a necessidade de previsão sobre direitos humanitários. No capítulo *Dignidade da pessoa humana como instrumento de humanização na execução penal: uma análise da efetividade dos diplomas internacionais no trabalho prisional brasileiro*,

[1] Período de 15 (quinze) anos em que Getúlio Dornelles Vargas governou o Brasil (1930-1945).

inserido no livro Direito Internacional dos Direitos Humanos e as pessoas em situação de vulnerabilidade, destacam-se três marcos importantes que inauguraram uma nova fase do direito internacional, mesmo antes da Segunda Guerra Mundial.

A fase do direito humanitário, a qual foi responsável por elaborar um conjunto de princípios e regras para limitar a violência durante o período de conflito armado. A segunda fase se deu logo após a Primeira Guerra Mundial (1914-1918), com a criação da Liga das Nações, responsável por limitar a autonomia estatal e aplicar sanções econômicas e militares aos Estados que violassem as regras existentes e, por fim, a terceira fase, que foi marcada pela criação da Organização Internacional do Trabalho (OIT), agência responsável pela elaboração de requisitos mínimos para proteção de trabalhadores (CORTEZ *et al.*, 2022, p. 464).

Contudo, foi somente diante das atrocidades cometidas pelas ordens opressoras na Segunda Guerra Mundial que a comunidade internacional sentiu a urgência em reforçar a proteção aos direitos humanos. Nesse contexto, Hanna Arendt (1989, p. 330) ressalta que só é possível perceber o "direito de ter direitos", quando milhões de pessoas perdem o mínimo que deveria ser assegurado por esses direitos e não podem mais recuperá-los. Ressalta, ainda, que "o direito de ter direitos, ou o direito de cada indivíduo pertencer à humanidade, deveria ser garantido pela própria humanidade" (ARENDT, 1989, p. 332).

O movimento humanístico, além de influenciar a edição de diplomas internacionais, como a Declaração Universal dos Direitos do Homem de 1948, também foi capaz de inspirar a elaboração da Constituição de 1946, resgatando os direitos fundamentais anteriormente previstos e recuperando, especialmente, as garantias da inviolabilidade do sigilo da correspondência e do domicílio (SILVA JÚNIOR, 2022, p. 156). Posteriormente, a Constituição de 1967, reformulada pela Emenda Constitucional nº 1, de 17 de outubro de 1969, manteve a existência de direitos e garantias, mas se tornou um texto meramente simbólico, uma vez que o país vivenciava um segundo momento sob domínio de um regime ditatorial[2].

Mais adiante, com a fragilidade do governo autoritário, o processo de democratização ganhou espaço no país. Os direitos fundamentais, até então tratados apenas de forma literal, ganharam força normativa no texto da Constituição de 1988 e além de resguardar os direitos fundamentais previstos nos outros ordenamentos, o constituinte acrescentou outros direitos no rol do artigo 5º da Constituição, como é o caso da inviolabilidade da intimidade, a vida privada, a honra e a imagem das pessoas (inciso X), ponto central desse estudo.

[2] Regime autoritário que teve início em 1964 e durou até o ano de 1985.

2.1 **Direitos fundamentais à luz da teoria do garantismo penal**

Em um contexto de desenvolvimento de direitos básicos inerentes aos seres humanos, foi preciso que o direito criminal se renovasse e passasse a servir a novos propósitos, de acordo com o desenvolvimento de cada sociedade e de seu respectivo ordenamento constitucional, mas sem alterar as bases estruturais da ciência criminal, firmadas na tradição jurídica do iluminismo e do liberalismo. As premissas encontradas nessa tradição, datadas do século XVIII, são diversas[3], mas destaque-se aqui aquela que aborda a limitação do poder punitivo e a tutela dos direitos fundamentais dos indivíduos contra as arbitrariedades praticadas pelos seus superiores hierárquicos (FERRAJOLI, p. 29, 2002).

Essas ideias foram consolidadas, especialmente, na obra *Dos delitos e das penas*, de Cesare Beccaria (1738-1794), o qual tornou-se símbolo da reação liberal diante da crueldade que o sistema penal vigente da época representava. Aos leitores de sua obra, Beccaria (1999, p. 23-24) declara inicialmente que "felizes as pouquíssimas nações que não esperaram que o lento movimento das combinações e vicissitudes humanas, após haverem atingido o mal extremo, conduzissem ao bem, mas que aceleraram as passagens intermediárias com boas leis", ressaltando, assim, que o objetivo de todas as nações deveria ser pautada na necessidade de conhecer as verdadeiras relações humanas e saber combater as irregularidades dos processos criminais através da elaboração de leis efetivas, sem aguardar que tais transformações ocorram somente após momentos de fragilidade.

Sobre o desenvolvimento das ciências, Beccaria (1999, p. 132) afirma ainda que "quem refletir sobre a história, em que certos intervalos de tempo se assemelham a períodos principais, encontrará mais vezes uma geração inteira sacrificada à felicidade das que a sucederam na enlutada", retratando a "necessária passagem das trevas da ignorância à luz da filosofia, da tirania à liberdade", uma vez que muitos foram os sacrifícios das sociedades anteriores ao tentar transformar o modelo tirano ainda existente em um modelo mais humanitário.

Diante disso, buscou-se um novo paradigma epistemológico para o enfrentamento da criminalidade, fazendo com que surgissem duas correntes de pensamento: o modelo garantista, fundada na percepção de limitação da pretensão punitiva com base na observância de direitos e

[3] Ferrajoli cita como exemplo as "doutrinas dos direitos naturais, as teorias contratualistas, a filosofia racionalista e empirista, as doutrinas políticas da separação dos poderes e da supremacia da lei, o positivismo jurídico e as concepções utilitaristas do direito e da pena" (2002, p. 29).

garantias constitucionais, e um modelo de características mais autoritárias que defendem a prevalência da pretensão acusatória em detrimento dos direitos do acusado.

A maioria dos países demonstraram afinidade à corrente garantista, mas é verdade que ainda existem discussões sobre utilizações de medidas mais autoritárias para crimes considerados mais graves, como é o caso de crimes de terrorismo (SILVA JÚNIOR, 2022, p. 24). Na América Latina, os pensamentos de Beccaria residiram na demonstração de forma sistemática das consequências da aplicação de suas ideias filosóficas no campo do controle social punitivo, trazendo como norte a obediência aos direitos mais básicos do ser humano (ZAFFARONI, 1989, p. 523), em evidente conformidade à corrente garantista.

Sem dúvida, os pressupostos teóricos e filosóficos de Beccaria colaboraram para a consolidação desses direitos nas constituições e codificações modernas, de forma que os diversos princípios garantistas se configuram como um esquema epistemológico, orientado a assegurar o "máximo grau de racionalidade e confiabilidade do juízo e, portanto, de limitação do poder punitivo e de tutela da pessoa contra a arbitrariedade" (FERRAJOLI, 2002, p. 30).

Em sua obra *Direito e razão*, Ferrajoli destaca três concepções do garantismo. A primeira designa um *modelo normativo de direito*, basicamente firmado sobre o princípio da estrita legalidade vinculado às premissas defendidas em um Estado de Direito. A segunda concepção define o garantismo como uma *teoria jurídica* que visa propiciar uma análise crítica sobre a validade e a efetividade das leis, além de uma consciência sobre as suas fontes de legitimação jurídica. Por fim, a terceira concepção trata sobre uma *filosofia política* que reflete basicamente a separação entre o direito e a moral na valoração do ordenamento jurídico, ou seja, impondo ao Direito e ao Estado o "ônus da justificação externa" (FERRAJOLI, 2002, p. 684-685). Portanto, unindo as três concepções destacadas, a teoria do garantismo penal pode ser compreendida como a defesa dos valores intrínsecos ao ser humano, colocando os direitos fundamentais e as garantias processuais acima das eventuais arbitrariedades cometidas.

Definido o conceito sobre a teoria garantista, faz-se necessário se ater ao exame dos direitos constitucionais fundamentais em espécie, uma vez que eles exigem, em um primeiro momento, a sua conceituação e distinção da terminologia de *garantias* constitucionais. Ruy Barbosa (1893) já pontuava a necessidade, a título de rigor científico, em diferenciar as terminologias *direitos* e *garantias*. Para o autor (1893, p. 193), "*direito*, 'é a faculdade reconhecida, natural, ou legal, de praticar, ou não praticar certos actos'. *Garantia,* ou *segurança* de um direito, é o requisito de legalidade, que o defende contra a ameaça de certas classes de atentados, de ocorrência mais ou menos fácil". Paulo Bonavides (2011, p. 525), esclarece que "existe a garantia sempre em face de um interesse que demanda proteção e de um perigo que

se deve conjurar", isto é, a garantia se coloca como um meio de defesa de direitos reconhecidos pelo constituinte.

Por outro lado, importante distinção sobre as expressões direitos humanos e direitos fundamentais também é ressaltada por Ingo Sarlet, Luiz Guilherme Marinoni e Daniel Mitidiero (2015). Inicialmente, os autores alertam a ausência de um consenso na esfera conceitual e terminológica dos termos utilizados, o que reforça a necessidade de se adotar uma terminologia única e adequada. Esclarecem, portanto, que "o termo 'direitos fundamentais' se aplica àqueles direitos (em geral atribuídos à pessoa humana) reconhecidos e positivados na esfera do direito constitucional positivo de determinado Estado", já os direitos humanos são considerados aqueles que guardam "relação com os documentos de direito internacional, por referir-se àquelas posições jurídicas que se reconhecem ao ser humano como tal, independentemente de sua vinculação com determinada ordem constitucional" (SARLET *et al*., 2015, p. 313-314).

Em face dessas constatações, reconhecer a diferença entre os dois conceitos abordados não significa desvincular os seus significados, muito pelo contrário. Os direitos humanos inseridos em diplomas internacionais, especialmente após a Segunda Guerra Mundial, foram alicerce para construção de vários ordenamentos constitucionais modernos, inclusive a Constituição Federal de 1988, logo, falar em direitos fundamentais é também falar sobre direitos de todos sob um viés garantista.

Acontece que o mundo está em constante transformação, o que significa que os direitos fundamentais, ora garantidos, deverão se adaptar às novas realidades. O advento da tecnologia como um "conjunto de saberes inerentes ao desenvolvimento e concepção dos instrumentos (artefatos, sistemas, processos e ambientes) criados pelo homem através da história para satisfazer suas necessidades e requerimentos pessoais e coletivos" (VERASZTO *et al*., 2009, p. 38), tem sido objeto de pesquisa de muitas ciências, inclusive a ciência criminal.

No mesmo sentido, é a obra *Tem futuro o direito penal*? de Claus Roxin, em que esclarece, de início, que a resposta para o questionamento que trouxe o título aos seus estudos não é tão simples de ser respondida, isso porque o direito penal ainda é uma instituição muito importante para assegurar a "paz infraestatal e uma distribuição de bens minimamente justa" (ROXIN, 2001, p. 460). Diante dessa realidade, Nucci (2016, p. 30) aponta a importância de realizar um "redimensionamento dos direitos humanos na era cibernética", ou seja, é preciso redefinir determinados direitos individuais, como o direito à liberdade e à intimidade, de forma a adequá-los a uma dimensão, ainda recente, que é "o mundo digital ou a vida virtual".

O conhecimento tecnológico e o desenvolvimento de recursos, como o *global positioning system* ou sistema de posicionamento global (GPS), tem se tornado grande

instrumento para uma série de atividades, seja ela de navegação aérea e marítima, meio ambiente, lazer ou até mesmo utilizada no âmbito da segurança pública e da investigação criminal (MONICO, 2000, p.15). Bustamante Donas (2001) traz ao mundo acadêmico a discussão sobre a necessidade de mudanças substanciais no que se refere aos direitos humanos no ambiente de novas tecnologias, o que seria, por ele considerado, a quarta geração de direitos humanos. Nas palavras do autor, "estas 'comunidades virtuales emancipadoras' marcan uma vía increíblemente fructífera hacia la promoción de derechos humanos de cuarta generación, a través de la transformación del conocimiento experto, la descentrazlización del saber y la potenciación de la ciudadanía[4]" (DUNAS, 2010, p. 8).

Exemplo prático dessa situação seria o caso do cometimento de crime contra o patrimônio, como o furto de um aparelho celular, em que fosse possível localizar o objeto através do sistema de posicionamento global (GPS). Se o aparelho estivesse em um ambiente doméstico, isto é, na residência de uma pessoa, seja do suspeito ou outro indivíduo, restaria evidente o conflito entre o direito à restituição patrimonial da vítima de furto e o direito à inviolabilidade de domicílio do detentor do objeto, o qual somente poderia sofrer flexibilização do seu direito constitucional através de autorização judicial, conforme veremos ao longo deste estudo.

Nesse ponto, não restam dúvidas de que o avanço da tecnologia, o advento da internet e o invento de novos instrumentos são considerados uma valiosa conquista da humanidade, porém, trouxe consigo questionamentos inevitáveis. Como assegurar segurança pública sem violar o direito à intimidade e à vida privada? Como ser eficiente no combate à impunidade à luz de direitos fundamentais? São indagações difíceis e complexas, porém necessárias.

2.2 **Ponderação dos direitos fundamentais relacionados ao processo penal**

A ocorrência de conflitos entre os direitos fundamentais assegurados ao longo da Constituição Federal, especialmente no que se refere ao processo penal, se tornou inevitável no decorrer da história. Não é raro acompanhar notícias de que os Tribunais Superiores precisaram se posicionar sobre a ocorrência de colisões entre direitos fundamentais básicos e qual deveria prevalecer. São discussões sobre liberdade de informação, a imagem do acusado e a presunção de inocência; a liberdade de expressão e a tutela da honra; a proibição de tortura ou de penas

[4] "Essas 'comunidades virtuais emancipatórias' marcam um caminho incrivelmente frutífero para a promoção dos direitos humanos de quarta geração, por meio da transformação do conhecimento especializado, da descentralização do conhecimento e do empoderamento da cidadania" (tradução nossa).

degradantes e a necessidade de aplicação de penas privativas de liberdade em ambientes carcerários inóspitos; a proibição de escravidão e o trabalho forçado, entre outros.

A título meramente exemplificativo, cita-se o Agravo Regimental no Recurso Extraordinário 1.292.275 do Rio de Janeiro, de relatoria do Ministro Dias Toffoli, em que foi discutida a divulgação de imagens de presos provisórios e a possibilidade de conflito normativo entre o direito à informação e o direito à intimidade. No caso concreto, foi proferida sentença de primeiro grau determinando a impossibilidade do poder estatal em divulgar imagens de presos provisórios, salvo se presente motivação prévia e idônea das razões imprescindíveis para exibição de imagens, ressaltando, especialmente, a utilidade dessa exposição para o processo penal. Portanto, o julgador, exercendo o papel de intérprete do caso, flexibilizou o direito fundamental à intimidade diante da necessidade e interesse estatal em exibir as imagens mencionadas.

Nesse caso, o voto do Relator destacou aplicação acertada da técnica de ponderação entre direitos fundamentais de mesma hierarquia, quais sejam, o direito à informação e o direito à intimidade. Tal fato se justifica pela inexistência de direitos fundamentais absolutos no ordenamento jurídico, fazendo com que caiba ao intérprete, em cada caso concreto, através de um juízo de ponderação, decidir qual direito fundamental deverá prevalecer. Situações semelhantes também foram mencionadas pelo Ministro, citando, por exemplo, a decisão nos autos do RE nº 612.687/DF-AgR sobre a relativização do direito à privacidade, na temática do sigilo bancário, diante dos interesses públicos, sociais e da justiça.

Apesar da pluralidade de decisões desta temática, percebe-se que o processo penal, em sua essência, retrata uma colisão de direitos fundamentais: o dever-poder de punir do poder estatal e o direito do investigado ou acusado em defender a sua liberdade. E a solução para essas colisões ou conflitos entre direitos fundamentais se faz mediante a utilização da técnica de ponderação[5], exigindo do poder judiciário, em regra, uma interpretação adequada dos direitos violados (SILVA JÚNIOR, 2021, p. 398). Logo, apesar da Constituição Federal insculpir um extenso rol de direitos e garantias fundamentais, colocando-os em posição de igualdade, isto é, sem impor qualquer hierarquização dos direitos ali previstos, é comum a existência de colisão entre esses direitos, sendo necessária a utilização de técnicas específicas para sua harmonização.

[5] A técnica de ponderação pode ser conceituada como uma "técnica de imposição na hipótese de antinomia entre direitos fundamentais, quando a aplicação de determinado direito fundamental aniquila, temporariamente, a validade expressa ou implicitamente de outro direito fundamental (GURGEL, 2018, p. 186).

Diante da possibilidade de colisão de direitos fundamentais, surgiram duas teorias que estudaram a temática de restrições a esses direitos: a teoria interna e a teoria externa. Para a teoria interna, defendida por Haberle, os direitos fundamentais possuem limites imanentes ao próprio direito e são insuscetíveis de ponderação, de modo que inexistiria qualquer restrição ao seu conteúdo (TORRES, 2009, p. 87). Desse modo, os direitos fundamentais poderiam ser equiparados à normativa das regras[6], uma vez que ou existiria um direito subjetivo a ser resguardado ou não. No caso da existência, esse mesmo direito somente poderia ser exercido dentro de seus limites.

A teoria externa, por outro lado, divide esse objeto anteriormente tratado como um só pela teoria interna, em dois: há, de um lado, o direito propriamente dito, e, de outro, as suas restrições. É, especialmente, a partir dessa distinção que é possível discutir sobre o sopesamento e a utilização da regra de proporcionalidade como forma de solução das colisões entre direitos fundamentais, isso porque é somente a partir dessa teoria que se compreende que as restrições, qualquer que seja a sua natureza, não têm qualquer influência no conteúdo do direito, podendo, apenas, no caso concreto, restringir o seu exercício (SILVA, 2017, p. 138).

No entanto, é importante distinguir a técnica de sopesamento ou ponderação e a aplicação da regra de proporcionalidade. A primeira pode ser identificada quando o legislador se vê obrigado a fazer um sopesamento entre dois ou mais princípios, sendo o resultado dessa técnica expressa em regra infraconstitucional. Em países que possuem uma jurisdição constitucional, como é o caso do Brasil, tal resultado pode ser questionado judicialmente através do controle de constitucionalidade da lei.

Ao longo desse processo ou de outras medidas judiciais que reflitam – mesmo que de forma reflexa – a colisão entre direitos fundamentais, o julgador deve-se recorrer à regra da proporcionalidade, isto é, se a regra infraconstitucional que restringe o direito fundamental é adequada a fomentar os objetivos ou outro direito fundamental; se não há outra medida eficiente e menos restritiva; e, por fim, se há um equilíbrio entre a restrição de um direito e a promoção do outro (SILVA, 2017, p. 178-179).

Nesse sentido, Robert Alexy demonstra a conexão existente entre a natureza dos princípios e a máxima da proporcionalidade, uma vez que a partir dos requisitos existentes na aplicação da regra da proporcionalidade – adequação, necessidade e proporcionalidade em sentido estrito – torna-se possível enquadrar os princípios como mandamentos de otimização

[6] O conflito entre regras somente pode ser resolvido se inserido uma cláusula de exceção que limite o conflito existente ou se pelo menos uma das regras for declarada inválida, isto é, ou a norma jurídica é válida, ou não é. Nesse caso, não há o que se falar sobre sopesamento ou ponderação (ALEXY, 2014, p. 92).

permitindo a sua aplicação em contextos fáticos e jurídicos diferentes (ALEXY, p. 2014, p. 92). Assim, enquanto as normas-regras demandam uma aplicação de validade ou não, as normas-princípios ordenam a sua aplicação dentro das possibilidades jurídicas existentes (GURGEL, 2018, p. 170).

Todavia, é imprescindível que a aplicação – seja da técnica de ponderação ou da regra de proporcionalidade – observe parâmetros mínimos de proteção contra a instrumentalização do indivíduo (GURGEL, 2018, p. 189). Para tanto, será utilizado como parâmetro o fundamento da dignidade da pessoa humana, de modo que compreender o seu conteúdo, como norma hierarquicamente superior a qualquer outra, e também resguardar a integridade do próprio ser humano contra abusos que possam ser eventualmente cometidos pelos intérpretes.

A dignidade da pessoa humana foi prevista pelo constituinte de 1988 como fundamento e valor primordial da República assegurado a todas as pessoas indistintamente, nos termos do inciso III do art. 1º, CF, de modo que não poderá sofrer qualquer alteração ou flexibilização, sob o risco de fomentar insegurança jurídica (NOVAIS, 2016, p. 39-40).

Para Gurgel (2018, p. 86), a dignidade da pessoa humana é acolhida no âmbito jurídico como "norma-princípio condutora de toda estrutura constitucional do Estado de direito", destacando, portanto, que a dignidade possui inúmeras funções no ordenamento jurídico brasileiro, quais sejam: fundamento, critério de interpretação, parâmetro de ponderação, além de cumprir importante papel de blindagem dos direitos fundamentais, ou seja, atuando como critério limitador dos limites dos direitos fundamentais. Moreira (2015, p. 93), assegura que os direitos humanos ao lado da dignidade humana são conceitos indispensáveis para a própria sociedade, mas muito mais do que discutir sobre o seu conceito, é necessária a sua concretização através de políticas públicas.

Desse modo, denota-se que a dignidade humana desenvolve diversas funções no ordenamento jurídico, sendo uma delas a de parâmetro de técnicas de sopesamento ou ponderação e da utilização da regra de proporcionalidade. Logo, entender esse fundamento ou princípio estruturante para os direitos fundamentais como conteúdo mínimo para solução da colisão entre outros direitos é o caminho mais seguro a ser traçado, uma vez que pensar o contrário seria equipará-lo a um direito fundamental, concordando com a ideia de que ela poderá ser ponderada diante de qualquer conflito narrado em uma situação concreta (CORTEZ, 2022, p. 462), o que levaria à insegurança do próprio direito postulado, como é o caso do conflito existente entre o direito à intimidade e à privacidade e o dever de proteção (eficiente).

2.2.1 Direito à intimidade e à privacidade *versus* o dever de proteção (eficiente)

A Constituição Federal de 1988 foi a primeira a reconhecer expressamente o direito à intimidade e à privacidade como bens jurídicos autônomos (art. 5º, X), mas isso não significa dizer que a *intimidade* e a *privacidade* estiveram sem guarida desde a Constituição Imperial de 1824. Em razão de as constituições anteriores incluírem o direito à inviolabilidade de domicílio e de correspondência em seu corpo normativo, o direito à intimidade e à vida privada acabaram sendo alcançados, já que a intenção incipiente do constituinte foi baseada na preservação da esfera privada ou íntima de uma pessoa diante das ingerências externas.

A Declaração Universal dos Direitos do Homem, de 1948, também não deixou de abordar a proteção do direito à intimidade e a privacidade, ao citar, em seu art. 12 que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda pessoa tem direito à proteção da lei", fazendo com que o direito à preservação de intimidade e da vida privada também estivessem respaldados por normativas internacionais.

No tocante à terminologia dos direitos de privacidade e de intimidade, é importante esclarecer que há quem considere essas duas expressões difíceis de serem diferenciadas, especialmente em virtude da associação entres esses direitos no próprio cotidiano (SARLET *et al.*, 2015, p. 457), já que na prática, o indivíduo dificilmente conseguirá separar o que seria a sua privacidade e o que pode ser considerado a sua intimidade. Entretanto, para fins de maior rigor científico, faz-se necessário buscar distinguir as nomenclaturas utilizadas pelo constituinte.

Nesse sentido, Ferraz Júnior (1993, p. 442) esclarece que a intimidade "é o âmbito do exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance de sua vida privada que, por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer em comum)". Na mesma linha, temos a conceituação dada por Silva Júnior (2022, p. 457), o qual aduz que "a intimidade possui duas dimensões: uma *interior* e outra *exterior*. Aquela se reveste de natureza física e material, recolhendo-se o homem ao seu *castelo* para desfrutar do sossego, enquanto esta se manifesta apenas no sentido psíquico", fazendo com que o direito à intimidade seja intrinsecamente ligado à condição humana.

O conceito de privacidade, por sua vez, nas palavras de Richard Posner (1978, p. 393) foi "*elusive and ill defined*[7]", isso porque muitos outros pesquisadores não obtiveram êxito ao

[7] "Elusivo e mal definido" (tradução nossa).

tentar definir o conceito de privacidade, mas o autor busca resolver esse problema de definição afirmando que um aspecto principal desse direito é simplesmente a retenção ou ocultação de informações. Já no estudo publicado por Warren e Brandeis (1890, p. 193), juízes da Suprema Corte dos Estados Unidos, asseveram que as mudanças políticas, sociais e econômicas acabam influenciando no reconhecimento de novos direitos, inclusive em suas definições, prova disso foi o direito à privacidade que antes garantia ao indivíduo suas terras e seus gados e com o tempo conseguiu atingir todas as formas de posse intangíveis, bem como tangíveis.

No âmbito brasileiro, Ferraz Júnior (1993, p. 442) conceituou *privacidade* como sendo aquela que "envolve a proteção de formas exclusivas *de convivência*. Trata-se de situações em que a comunicação é inevitável (em termos de relação de alguém com alguém que, entre si, trocam mensagens), das quais, em princípio, são excluídos terceiros". Para Silva Júnior (2022, p. 465), apesar da "garantia da vida privada ser uma variante do direito à intimidade", elas não se confundem, já que a vida privada "diz respeito à proteção à vida pessoal e familiar da pessoa, que tem o direito ao sossego e de não ter a sua vida investigada e revelada ao bel-prazer das outras".

Em sua obra, André de Carvalho Ramos (2019, p. 1100) pontua a existência de uma teoria das esferas ou círculos concêntricos. Com base nessa teoria, seria possível entender a dinâmica de proteção à privacidade através de três círculos concêntricos: a vida privada em sentido estrito, o círculo da intimidade e o círculo do segredo. O primeiro refere-se às informações materiais e de difícil acesso, como dados fiscais, bancários ou telemáticos, por exemplo. No círculo da intimidade, por sua vez, estariam contidas informações compartilhadas apenas com familiares e amigos próximos. Aqui, o autor aponta que estariam inseridas a previsão de inviolabilidade de domicílio e a proteção do acesso indevido e publicização do conteúdo abordado. O último círculo, o do segredo, compila informações íntimas e confidenciais do titular, envolvendo opções e sentimentos individuais.

Dessa forma, é possível compreender que o direito à privacidade é oriundo do próprio comportamento do seu titular, fazendo com que o indivíduo possa optar por flexibilizá-lo diante dos seus interesses. Exemplo disso, no âmbito tecnológico, é a adesão às redes sociais, espaços criados no mundo virtual em que o sujeito poderá compartilhar informações pessoais ou profissionais, além de conhecimento sobre algum tema específico. Para Tomaél *et al*. (2005, p. 94), as redes sociais passaram a ser utilizadas não só para objetivos acadêmicos ou científicos, mas também conquistou outros adeptos, muitas vezes, apenas pelo prazer de desenvolver uma rede de relacionamentos. Logo, o cuidado com o compartilhamento de informações pessoais

pode ser deixado de lado, por simples opção do indivíduo quando o objetivo é ampliar a sua rede de contatos.

Em sentido oposto, foi o exemplo trazido por André de Carvalho Ramos (2019, p. 1105) ao relembrar um caso julgado pela Corte Europeia de Direitos Humanos (Corte EDH), envolvendo a Princesa Caroline de Mônaco, alvo frequente de fotógrafos conhecidos como *paparazzi*, os quais, muitas vezes, comercializavam as fotografias retiradas durante o cotidiano da Princesa. Por mais que fosse considerada uma figura pública, optando por flexibilizar a sua privacidade em ambientes públicos, a Corte considerou que houve violação ao direito à privacidade, previsto na Convenção Europeia de Direitos Humanos, diante da ausência de interesse público legítimo e da falta de autorização da Princesa.

Nesse ponto, é possível indagar se o dever de proteção aos direitos à intimidade ou à privacidade caberia exclusivamente aos seus portadores ou também poderia ser considerada uma responsabilidade do Estado. Julie E. Cohen (2013, p. 1927), professor da Universidade de Direito de Georgetown, em um artigo publicado na Revista *Harvard Law Review*, destacou que o direito à privacidade não deve ser compreendido simplesmente como um direito individual, isso porque a privacidade promove objetivos fundamentais de políticas públicas relacionado ao um estado democrático de direito, a inovação e ao próprio desenvolvimento humano, e esses fins devem ser levados em consideração.

É uníssono o fato de que as novas tecnologias têm influenciado na adequação de um novo direito, assim como têm influenciado na nova estruturação do direito à intimidade e à privacidade. Seja do lado dos agentes estatais de segurança pública ou do lado dos cidadãos, a verdade é que a busca por um equilíbrio entre a proteção (eficiente) e os limites da atuação do Estado é constante.

Nesse sentido, percebe-se que a discussão sobre vigilância trazida por Foucault em sua obra *Vigiar e punir* permanece atual, isso porque o equilíbrio que hoje se busca entre o direito à segurança pública e os limites estatais continua sendo objeto de discussão nos tribunais e no mundo acadêmico. O caso da transição das penas como forma de suplício para aplicação de penas privativas de liberdade em ambientes de vigilância ininterrupta seria um exemplo dessa discussão, uma vez que a permanente visibilidade dos detentos facilitaria o acompanhamento da funcionalidade do poder estatal, mas ao mesmo tempo colocaria o indivíduo em uma posição de instrumentalidade ou de docilidade (FOUCAULT, 2004, p. 166).

A ideia de Foucault foi corroborada através do modelo panóptico, concebido por Bentham, em 1787. Esse modelo foi baseado na realização de inspeção em qualquer estabelecimento, sem exceção, mas esse local não poderia ser tão extenso para que pudesse ser

controlado ou dirigido a partir de edifícios, de modo a manter sob vigilância um determinado número de pessoas. O autor defendia que quanto maior a inspeção, mais perfeitamente o propósito de qualquer estabelecimento a ser aplicado tal modalidade seria alcançado, isto é, seja qual for o propósito elencado – "punir o incorrigível, encerrar o insano, reformar o viciado, confinar o suspeito, empregar o desocupado, manter o desassistido, curar o doente..." (BENTHAM, 2008, p. 19) – quanto mais constante as pessoas forem inspecionadas mais fácil seria atingir o objetivo traçado inicialmente.

Para Foucault (2004, p. 165) o panóptico seria, em um breve resumo, conhecido basicamente por sua construção em formato de anel em que no centro há uma torre; esta seria composta por janelas amplas que se abrem sobre a face interna do anel, permitindo uma visibilidade completa do estabelecimento e assegurando o funcionamento automático do poder. Acontece que apesar dos autores defenderem que o sistema de vigilância ininterrupta em qualquer ambiente ensejaria um controle e uma auto regulação das condutas do indivíduo monitorado, impulsionando a discussão sobre o monitoramento, não foi nesse momento discutido o impacto dessa hiper vigilância na própria sociedade.

Uma amostra do tratamento sobre o direito à privacidade e à intimidade no âmbito público e constitucional atual, foi a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 722, do Distrito Federal, julgado procedente, por maioria, pelo plenário do Supremo Tribunal Federal (STF), em 16 de maio de 2022. No caso, foi declarada a inconstitucionalidade dos atos praticados pelo Ministério da Justiça e Segurança Pública (MJSP) de produção e compartilhamento de dossiê contendo informações sobre a vida pessoal de um grupo de 579 (quinhentos e setenta e nove) servidores públicos federais e estaduais, além de professores universitários, integrantes de chamado "movimento antifascismo".

Confirmada a medida cautelar anteriormente deferida, por unanimidade, o Tribunal Constitucional foi palco para o debate sobre violações a diversos preceitos fundamentais previstos no art. 5º da Constituição, entre eles, o direito à intimidade e à vida privada. Nesse ponto, chama atenção o voto proferido pela Ministra Rosa Weber, em sede cautelar, o qual destacou ponto específico para tratar sobre a lesão à intimidade, à vida privada, à honra e à imagem. Em seu voto, a Ministra ressaltou que "a facilidade com que a privacidade será protegida ou exposta transforma-se à medida em que evoluem as tecnologias da informação e da comunicação".

Trazendo essa discussão para os dias atuais, temos as palavras da Min. Rosa Weber, a qual aduz que "A Constituição da liberdade não acolhe a vigilância pela vigilância", isto é, em casos concretos, como o analisado pelo Supremo Tribunal Federal, deve restar comprovado

interesse legítimo a justificar restrições aos direitos individuais, o que não foi o caso da ADPF nº 722. Nessa perspectiva, Silva Júnior (2022, p. 216) aponta que, havendo justificativa plausível, é possível a flexibilização de qualquer direito fundamental em decorrência da proteção da ordem pública e do exercício da atividade policial ostensiva. Logo, mesmo o direito à intimidade e à vida privada sendo bens protegidos pelo constituinte, eles não são absolutos, mas a justificativa para sua relativização deve ser ponderada diante do caso concreto.

O autor menciona, como exemplo, o caso da interceptação de carta-bomba por autoridade policial, sem autorização judicial, com o objetivo de evitar a ocorrência de um crime grave já que a sua abertura poderia ocasionar em uma explosão. Apesar de não se proceder a abertura desse documento, por motivos óbvios, cumpre notar que, na eventualidade do agente policial necessitar abri-la, não seria esse ato caracterizado como ilegal, isso porque restaria justificada a necessidade de relativização do direito fundamental à inviolabilidade de correspondência em virtude da proteção à segurança pública (SILVA JÚNIOR, 2022, p. 508-509). Dessa forma, não seria razoável considerar todo direito absoluto e inabalável, sob pena de colocar em risco a própria sobrevivência da sociedade.

É por esse ângulo que é possível encontrar o dever de proteção atribuído ao Estado, "no sentido de que a este incumbe zelar, inclusive preventivamente, pela proteção dos direitos fundamentais dos indivíduos não somente contra os poderes públicos, mas também contra agressões oriundas de particulares e até mesmo de outros Estados" (SARLET, 2006, p. 330). Exemplo prático dessa afirmação encontra-se no voto do Ministro Gilmar Mendes na Ação Direta de Inconstitucionalidade (ADI) nº 3112, do Distrito Federal, de relatoria do Ministro Ricardo Lewandowski, que tratou sobre a inconstitucionalidade do Estatuto do Desarmamento, consubstanciado na Lei nº 10.826, de 22 de dezembro de 2003.

Em seu voto, o Ministro ressaltou que "os direitos fundamentais não podem ser considerados apenas como proibições de intervenção (*Eingriffsverbote*[8]), expressando também um postulado de proteção (*Schutzgebote*[9])", isto é, não se pode falar apenas de proibição do excesso, mas deve ser dado igual importância à proibição de proteção insuficiente. Com base na Constituição Alemã, o dever de proteção pode ser classificado em três formas: a primeira é o dever de proibição (*Verbotspflicht*[10]), ou seja, o dever de proibir determinada conduta; a segunda forma é o dever de segurança (*Sicherheitspflicht*[11]), o qual impõe ao Estado o dever de

[8] Proibições de intervenção (tradução nossa).
[9] Regras de proteção (tradução nossa).
[10] Dever de proibição (tradução nossa).
[11] Dever de segurança (tradução nossa).

proteger o indivíduo contra ataques de terceiros e a última forma é o dever de evitar riscos (*Risikopflicht*[12]), o qual autoriza o poder público a adotar medidas de proteção ou de prevenção, especialmente com base no desenvolvimento tecnológico, visando evitar riscos ao cidadão (MENDES, 2004, p. 141).

Por esse ângulo, Silva Júnior (2022, p. 224-225) destaca que no âmbito do exercício da pretensão punitiva, como resultado do dever de proteção (eficiente) do Estado, "é preciso que sejam adotadas medidas adequadas e com certo grau de eficiência para que, nessa perspectiva, sejam preservados/concretizados os direitos fundamentais". Assim, não basta que o poder estatal exerça um dever de proteger o indivíduo contra eventuais ataques, é necessário que essa proteção seja, de fato, eficiente, no sentido de resguardar direitos essenciais ao desenvolvimento do ser humano.

Com base no estudo entre o dever de proteção (eficiente) e a vedação de uma pretensão punitiva desarrazoada, emerge a teoria do garantismo penal, de Luigi Ferrajoli, usado como instrumento de proteção aos direitos fundamentais. Tradicionalmente, por essa teoria busca-se a diminuição da pretensão punitiva estatal em detrimento da proteção de direitos fundamentais individuais. Acontece que esse conceito incipiente, baseado em uma acepção negativa, ajustada à defesa apenas de direitos fundamentais individuais no âmbito de um Estado Liberal de Direito, não foi o suficiente para o desenvolvimento de um Estado Democrático de Direito, isso porque por mais que seja indispensável a proteção às liberdades individuais, a ordem constitucional também prevê outros direitos e deveres constitucionais igualmente dignos de proteção (DE ANDRADE CORDEIRO *et al*., 2021, p. 133).

Essa necessidade da teoria garantista proteger não só os direitos fundamentais individuais, mas todos aqueles previstos em nosso ordenamento constitucional, corrobora uma visão positiva da teoria de Ferrajoli, consistente no "dever prestacional do Estado de salvaguardar os mais caros bens jurídicos fundamentais de seus cidadãos em face de ataques intoleráveis e ilícitos praticados por terceiros" (DE ANDRADE CORDEIRO *et al*., 2021, p. 134). Nessa lógica, em sede do Habeas Corpus nº 102.087, de Minas Gerais, o relator e Ministro Celso de Mello, expôs que "os direitos fundamentais expressam não apenas uma proibição do excesso (*Übermassverbote*[13]), como também podem ser traduzidos como proibições de proteção insuficiente ou imperativos de tutela (*Untermassverbote*[14])".

---

[12] Dever de risco (tradução nossa).
[13] Excesso de proibições (tradução nossa).
[14] Proibições de tamanho menor (tradução nossa).

Na relação entre os direitos humanos e o direito criminal, destaca-se que "em um Estado Democrático de Direito, o Poder Público não pode se omitir na promoção dos direitos humanos, devendo protegê-los inclusive com instrumento penal" (RAMOS, 2019, p. 1248). Logo, na eventualidade do poder estatal não cumprir com o seu dever de proteção eficiente, estar-se-á violando tanto a Constituição Federal como também os tratados de direitos humanos que já foram ratificados pelo Brasil. Assim, se por um lado, o poder estatal deve exercer a sua pretensão punitiva buscando coibir o cometimento de crimes, ele também deve prever mecanismos para coibir os seus próprios excessos e proteger a sociedade das violações dos seus bens jurídicos mais preciosos, como é o caso do direito fundamental à intimidade e à privacidade.

No entanto, compatibilizar esses direitos fundamentais com o dever de proteção (eficiente) por parte do ente estatal não tem sido uma tarefa fácil. Atualmente, o desenvolvimento de novas tecnologias e a elaboração de novas políticas públicas tem exigido uma visão dinâmica e criativa capaz de preservar os direitos constitucionalmente afetados. Nesse sentido, Cohen (2013, p. 1933) ressalta que "*that privacy is important and urgently in need of preservation, and that current regulatory strategies seem unlikely to prove up to the task*[15]", ou seja, é inquestionável que o direito à privacidade precisa ser preservado e que as atuais estratégias normativas parecem não estar à altura dessa tarefa.

Silva Júnior (2022, p. 225) consolida esses entendimentos ao afirmar que na medida em que o dever de proteção impõe a existência de instrumentos vinculados aos três poderes – legislativo, executivo e judiciário – capazes de concretizar os direitos fundamentais resguardados por nossa Constituição, "a proibição de proteção insuficiente, oriunda do princípio da proporcionalidade, reclama que esses instrumentos sejam hábeis e eficazes no amparo ao desempenho dessa função estatal".

Então, a partir da indispensabilidade de instrumentos normativos necessários a proteção de direitos fundamentais, surge a necessidade de aprofundar os estudos em relação ao próprio conteúdo normativo, incluindo os limites que a autoridade pública deverá observar, a fim de exercer a sua função/dever de proteção (eficiente), no que diz respeito à preservação do direito à intimidade e à privacidade, especialmente no que se refere à proteção dos dados pessoais no âmbito criminal.

---

[15] "A privacidade é importante e precisa ser preservada com urgência, e que as estratégias regulatórias atuais parecem improváveis de cumprir a tarefa" (tradução nossa).

2.2.2 Direito à proteção dos dados pessoais no âmbito da segurança pública e investigação criminal

No campo de proteção à intimidade e à vida privada, também se encontra a preservação ao sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, nos termos do art. 5º, inciso XII da Constituição Federal, além do sigilo de informações pessoais, fiscais e bancárias que apesar de não estarem expressos na Constituição, são desdobramentos evidentes dos direitos fundamentais ora analisados.

Uma das principais implicações da violação desses direitos no âmbito criminal é a inutilização da prova que poderá ser considerada ilícita, salvo se houver autorização judicial para fins de investigação criminal ou instrução processual penal, nos termos do art. 5º, inciso XII, da Constituição Federal. No entanto, por força do desenvolvimento e da utilização de novas tecnologias na seara penal, a proteção, especialmente aos dados pessoais, acaba gerando dúvidas interpretativas, merecendo, uma reflexão mais aprofundada.

A disciplina jurídica sobre a proteção de dados pessoais remete aos estudos de, pelo menos, cinco décadas, sendo a Lei de Proteção de Dados do *Land* alemão de Hesse, de 1970, o primeiro diploma normativo a tratar sobre esse conteúdo (DONEDA, 2022, p. 30). O aumento exponencial na produção e processamento de dados relacionados à esfera privada dos indivíduos ao longo do tempo se tornou um fator de risco ao indivíduo, fazendo com que a exposição dos seus dados pessoais pudesse violar os direitos mais básicos do ser humano. Assim, desde o momento que o controle e regulação desses dados se tornaram primordiais à proteção da tutela integral da pessoa, passou-se ao fortalecimento da elaboração de normatizações capazes de regular o processamento desses dados.

Danilo Doneda (2022, p. 39-40) esclarece que a história da proteção de dados pessoais no Brasil também teve início na década de 1970, em que pese o seu desdobramento técnico não ter sido exitoso. O autor cita o projeto do Registro Nacional de Pessoas Naturais (RENAPE), o qual previa a criação de um banco de dados e de um órgão com abrangência nacional, mas que acabou sendo arquivado em 1978, servindo de inspiração para um projeto de lei, de autoria do Deputado Faria Lima, com o mesmo objetivo. Além desse, destaca também a criação do projeto de Lei nº 2.796, de 1980, de autoria da Deputada Cristina Tavares, que tinha como objetivo assegurar aos cidadãos o acesso às suas informações que estivessem localizadas em um banco de dados. O projeto também foi arquivado, mas acabou influenciando na introdução do instrumento de *habeas data* na Constituição brasileira de 1988.

A nova garantia constitucional conhecida como *habeas data* foi inserida no inciso LXXII, no art. 5º da Constituição, e foi concedida para "assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter pública" e ainda "para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativos", segundo dispõe literalmente a regra constitucional.

Nas palavras de Bonavides (2011, p. 553), o remédio constitucional "cristaliza historicamente na consciência da sociedade brasileira uma reação jurídica do constituinte a violações, manipulações e excessos perpetrados em matéria informativa pessoal pelas entidades governamentais da ditadura ao longo de duas décadas". O início dessa discussão sobre proteção de dados gerou, no direito interno, a necessidade de normatização. Um dos primeiros diplomas a inserirem alguma forma de anteparo às garantias constitucionais de privacidade e intimidade, foi o Código de Defesa do Consumidor (CDC).

A Lei nº 8.078, de 11 de setembro de 1990, a qual dispõe sobre a proteção do consumidor, inseriu em seu art. 43 a previsão de bancos de dados e também do cadastro de consumidores que poderiam ter acesso às suas informações, exigindo, inclusive, a correção de eventuais informações incorretas. Outra legislação de suma importância para o fortalecimento dessas normativas foi a criação da Lei de Acesso à Informação (Lei nº 12.527/2011), que previu uma seção para tratar sobre as informações pessoais e o acesso restrito a agentes públicos legalmente autorizados, reconhecendo a primordialidade em proteger os dados pessoais mesmo em uma legislação destinada à transparência (DONEDA, 2022, p. 43).

As transformações resultantes do uso nas novas tecnologias por indivíduos, que ainda não sabiam como se comportar nessa esfera virtual, vieram acompanhadas de incertezas no mundo jurídico. O Direito Criminal, compreendido como direito penal e processual penal, se viu diante de um espaço relativamente novo, no qual não se encontrava mais fronteiras apenas físicas, como era historicamente familiarizado, mas também virtuais.

Ao mesmo tempo, essa era uma preocupação mundial, uma vez que diversos governos, inclusive o brasileiro e o alemão, eram vítimas de espionagem, o que levou à elaboração do projeto intitulado "O direito à privacidade na era digital" (United Nation, 2003) e encaminhamento à Organização das Nações Unidas, reafirmando-se o direito à privacidade, disposto no art. 12 da Declaração Universal dos Direitos Humanos e pelo art. 17 do Pacto Internacional de Direitos Civis e Políticos, diante do uso das novas tecnologias de informação por pessoas, empresas e governos na vigilância, interceptação e processamento desses dados (TOMASEVICIUS FILHO, 2016, p. 272)

Em 23 de abril de 2014, a Lei nº 12.965, conhecida como Marco Civil da Internet, veio com o objetivo de estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Apesar de disciplinar o uso da internet com base na preservação de direitos como a inviolabilidade da intimidade e da vida privada, o Marco Civil não apresentou efeitos práticos. De acordo com Eduardo Tomasevicius Filho (2016, p. 279), são muitas as deficiências e insuficiências do Marco Civil da Internet, mas o primeiro ponto que merece destaque é a falta de inovação do ordenamento jurídico, uma vez que o legislador acabou sendo redundante em várias disposições, repetindo o que já consta na Constituição Federal, como é o caso da inviolabilidade da intimidade, do sigilo e do direito à liberdade de expressão.

Quatro anos após a vigência do Marco Civil, foi publicada a Lei nº 13.709, de 14 de agosto de 2018, dispondo sobre a Lei Geral de Proteção de Dados Pessoais (LGPD), mas trazendo uma ressalva quanto à sua aplicabilidade no âmbito da segurança pública e das atividades de investigação e repressão de infrações penais, na forma do art. 4º, inciso III, alíneas "a" e "d", isto é, as previsões ali contidas não poderiam ser aplicadas na área criminal. O objetivo desse tópico é, portanto, analisar a proteção de dados pessoais nessa seara e explorar o significado desse recorte legislativo.

Com capítulo próprio na Constituição Federal, a segurança pública pode ser entendida como dever do Estado, direito e responsabilidade de todos, visando a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, a ser exercida através da polícia federal, polícia rodoviária federal, polícia ferroviária federal, polícias civis, polícias militares e corpos de bombeiros militares, além de polícias penais federal, estaduais e distrital, nos termos do art. 144. De lima *et al*. (2013, p. 62) entende que o conceito de segurança pública pode apresentar dois significados, por um lado, a preservação da ordem pública como forma de acautelamento do meio social e, por outro, a incolumidade das pessoas e do patrimônio, isto é, afastar do perigo e manter a sociedade e o patrimônio ilesos e bem conservados.

Em contrapartida, a investigação criminal é uma atividade pós-delitiva, isto é, após o cometimento do fato típico penal, surge para o Estado o dever de investigação e persecução penal para fins de comprovar a existência de um crime. Para Braz (2013), "o objecto da investigação criminal incide sobre factos (acções ou omissões) e sobre o comportamento humano que os originou, ou seja, sobre a materialidade e autoria do ilícito criminal". Assim, podemos vislumbrar a investigação criminal como um procedimento destinado a buscar maior proximidade com a verdade real dos fatos, a fim de demonstrar a realização de determinado crime e a sua autoria.

No plano normativo, a Lei nº 12.830, de 20 de junho de 2013, a qual dispõe sobre a investigação criminal conduzida pelo delegado de polícia, traz como objetivo da investigação criminal a apuração das circunstâncias, da materialidade e da autoria das infrações penais, cabendo ao agente competente a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos, nos termos do art. 2º. Concomitantemente, o Código de Processo Penal, de 1941, dispõe que o inquérito policial terá por fim a apuração das infrações penais e da sua autoria, nos termos do seu art. 4º.

Como forma de exemplificar a relação de proteção de dados no âmbito de investigações criminal, temos o julgamento realizado no dia 23 de fevereiro de 2023, da Ação Declaratória de Constitucionalidade nº 51, do Distrito Federal, e de Relatoria do Ministro Gilmar Mendes. O caso concreto foi pautado em um pedido da Federação das Associações das Empresas de Tecnologia da Informação (Assespro Nacional) pelo reconhecimento da constitucionalidade do Decreto Federal nº 3.810/2001, que dispõe sobre o Acordo de Assistência Judiciário-penal firmado entre o Brasil e os Estados Unidos (Mutual Legal Assistance Treaty – MLAT), o art. 237, inciso II, do Código Processual Civil (CPC), que trata sobre a expedição de carta rogatória e dos arts. 780 e 783 do CPP, que dispõem sobre a homologação de sentenças penais estrangeiras e sobre cartas rogatórias, respectivamente.

Com base no pedido inicial, o Poder Judiciário ao requisitar diretamente informações ou dados sobre empresas de tecnologias sediadas no exterior estaria violando esses dispositivos. No entanto, o Supremo Tribunal Federal entendeu que os juízes brasileiros podem determinar a requisição direta desses dados às empresas de tecnologias internacionais, conforme o art. 11 do Marco Civil da Internet, o qual dispõe sobre a aplicação da legislação brasileira nas operações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações, desde que pelo menos um desses atos ocorra em território nacional.

Nesse mesmo sentido, o Superior Tribunal de Justiça, nos autos do Recurso Ordinário em Mandado de Segurança (RMS) nº 66.392 do Rio Grande do Sul, de Relatoria do Ministro João Otávio de Noronha, julgado em 16 de agosto de 2022, entendeu que “empresas que prestam serviços de aplicação na internet em território brasileiro devem necessariamente se submeter ao ordenamento jurídico pátrio, independentemente da circunstância de possuírem filiais no Brasil e/ou realizarem armazenamento em nuvem”. Logo, não foi utilizado da cooperação jurídica internacional nesse caso, em virtude da morosidade, dando-se prioridade à solicitação direta de dados das empresas de tecnologia.

Outra regra utilizada para dar embasamento às solicitações diretas pelo Poder Judiciário, foi a Convenção sobre o Crime Cibernético, conhecida como Convenção de

Budapeste, incorporada ao Brasil em 17 de dezembro de 2021 sob a forma do Decreto Legislativo nº 37. O art. 18 da referida norma trata sobre a possibilidade das autoridades competentes ordenarem a uma pessoa ou a um fornecedor de serviços a comunicação sobre dados informações específicos na sua posse ou sob o seu controle, corroborando o art. 11 do Marco Civil da Internet. Diante desse julgamento, percebe-se que os Estados têm criado estratégias para facilitar a requisição de informações ou dados pessoais localizados em servidores de tecnologia a fim de superar as dificuldades impostas por normativas de cooperação jurídica internacional que acabam dificultando a efetiva resolução de uma investigação criminal diante do enorme lapso temporal que é despendido com o cumprimento de todas as regras.

No entanto, em que pese a coleta de dados pessoais ser fator de suma importância para o desenvolvimento de uma política de segurança pública ou até mesmo para a conclusão de uma investigação criminal, é necessário que pontuar que a requisição de dados pessoais realizadas de forma irrazoável pode ferir diretamente direitos fundamentais. Assim, é imprescindível que se estabeleça uma série de critérios para o regular tratamento desses dados sensíveis.

A Alemanha foi um dos primeiros países a editarem uma lei sobre proteção de dados, conhecida como *Bundesdatenschutzgesezt*[16], editada em 1970 pelo Parlamento alemão. No entanto, o ápice do reconhecimento da proteção de dados se deu com o julgamento sobre o censo demográfico que estava ocorrendo no país no ano de 1983. Influenciado, entre outras razões, pelas previsões publicadas no livro 1984, de George Orwell, que chamava atenção dos leitores para a existência de uma vigilância estatal, os cidadãos alemães protestavam sobre o levantamento de diversos dados pessoais, e não só do número de habitantes. Com isso, através de diversas reclamações constitucionais, o Tribunal Constitucional Federal suspendeu os efeitos da lei federal que regulamentava o censo e estabeleceu o direito fundamental à autodeterminação informativa (*Grundrecht auf informationelle Selbsbestimmung*[17]) (MENKE, 2019, p. 782-784).

De acordo com o Tribunal Constitucional da Alemanha, o novo direito fundamental, derivado do direito da personalidade, foi estruturado com base em três pilares. O primeiro pilar do direito da autodeterminação informativa seria o direito do indivíduo em poder decidir, ele próprio, sobre a coleta e a utilização de informações de cunho pessoal. A segunda seria basicamente pautada na flexibilidade do teor de proteção, garantindo, assim, o direito do

[16] Lei Federal de Proteção de Dados (tradução nossa).
[17] Direito fundamental à autodeterminação informacional (tradução nossa).

indivíduo permanecer em sua esfera íntima sem intromissões indevidas e, por último, se encontra a proteção aos registros pessoais coletados (MENDES, 2020, p. 12).

Entretanto, para fins desse estudo, destaca-se um outro capítulo da história do Tribunal Constitucional Federal da Alemanha: o reconhecimento do direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais (*Grundrecht auf Gewahrleistung der Vertraulichkeit und Integritat informationstechnisher Systeme*[18]). Esse direito foi reconhecido através de um julgamento, no ano de 2008, em que se analisou uma reclamação constitucional contra dispositivos da lei do Estado do Nordrhein-Westfalen, a qual regulamentava e permitia a busca ou investigação remota de computadores de pessoas suspeitas de cometerem ilícitos criminais (MENKE, 2019, p. 782).

Para Joelsons (2021, p. 14), esse mais recente direito fundamental seria apto a "proteger a vida pessoal e privada dos titulares de direitos no acesso a dispositivos de tecnologia da informação e, em particular, contra o acesso do estado ao sistema de tecnologia da informação como um todo", ou seja, o objetivo da instituição desse direito reside na proteção ao próprio sistema informático pessoal. No entanto, o Tribunal Constitucional Alemão ao mesmo tempo que reconheceu e preservou o direito à proteção de dados pessoais, também se preocupou em estabelecer exceções tanto para fins preventivos, quanto para persecução penal.

Dessa forma, o Tribunal tratou sobre as limitações e requisitos para a restrição desse mais novo direito fundamental. Como primeiro requisito, estaria a obediência à reserva de lei, sendo necessária a existência de lei especial para que se possa restringir o direito resguardado. Menke (2019, p. 801) esclarece que "o texto legal deve ainda estar de acordo com os postulados da clareza da precisão normativas bem assim com a proporcionalidade, contemplando a adequação (*Geeignetheit*), necessidade *(Erforderlichkei*) e proporcionalidade em sentido estrito (*Verhältnismäßigkeit im engeren Sinn*)".

O segundo requisito, de cunho material, é relacionado à finalidade da obtenção dos dados, ou seja, é preciso que haja um objetivo determinado pelo poder estatal ao buscar coletar dados de cunho pessoal dos cidadãos, mesmo que isso seja direcionado ao âmbito criminal. Nesse ponto, é preciso que que seja viável determinar quais pessoas estão envolvidas como eventuais suspeitas do cometimento de um fato típico, sendo as informações coletadas diretamente relacionados com a investigação, de modo que o direito de terceiros não envolvidos não seja violado. Por fim, o Tribunal exige que a autorização desse monitoramento seja através de ordem judicial, isso porque o poder judiciário seria o único competente e neutro a conseguir

[18] Direito fundamental à confidencialidade e integridade dos sistemas de tecnologia da informação.

sopesar os interesses do suspeito, em face de medidas tão invasivas. (MENKE, 2019, p. 803-804).

Nesse sentido, extrai-se da jurisprudência alemã a importância em analisar o monitoramento de determinadas informações na área de segurança pública e da persecução penal, mas também o cuidado com a ideia de um capitalismo informacional. Não é possível deixar de lado ideais iluministas de proteção ao ser humano e de seus direitos fundamentais, sob pena de reduzir a ciência criminal à um instrumento autoritário e antigarantista, modelo incompatível com um estado democrático de direito.

É verdade que o desenvolvimento do assunto no Brasil tem se dado de forma tardia quando comparado a outros modelos internacionais. Exemplo disso é que o direito à proteção de dados pessoais, inclusive nos meios digitais, só foi inserido como direito e garantia fundamental no ano de 2022, através da Emenda Constitucional nº 115, de 10 de fevereiro, o qual estabeleceu também como competência privativa da União a legislação sobre proteção e tratamento dos dados pessoais. Porém, isso não significa que a importação de um modelo alemão seria imprescindível à realidade brasileira. Faz-se necessário ter em mente que em cada lei há muitas regras específicas e atreladas à realidade vivenciada, muitas vezes até de difícil manuseio, mas os julgados e legislações, sem dúvidas, representará um marco para contribuição do desenvolvimento das questões de proteção de dados pessoais no âmbito da segurança pública e na investigação criminal no Brasil.

3 A PROVA DIGITAL NO PROCESSO PENAL BRASILEIRO

O Direito, como reflexo da realidade de cada sociedade, passou por muitas transformações ao longo do tempo. Da época do direito canônico, em que o poder estava concentrado na Igreja, e da era industrial, que o instrumento de poder era o capital monopolizado pelo Estado, transpomos para a era digital, em que o instrumento de poder é a própria informação (PINHEIRO, 2021, p. 46). Ocorre que esse poder informacional está diretamente associado ao avanço da tecnologia, isso porque desde o surgimento da internet[19] na segunda metade do século XX, houve uma potencialização do acesso à informação através de meios eletrônicos (MINTO, 2021, p. 19).

O avanço da tecnologia possibilitou a transmissão dessas informações através de uma rede de comunicação que pode ser acessado e armazenado em qualquer lugar, a qualquer tempo e em questões de minutos, com um único clique (BLAGITZ DE ABREU E SILVA, 2017, p. 116). Dessa forma, a utilização de internet, computadores, *smartphones* e tantos outros equipamentos de comunicação possibilitaram o compartilhamento de informações de forma instantânea para qualquer parte do globo, fazendo com que o poder informacional se tornasse o principal responsável da sustentação econômica de um Estado soberano.

Com o fim de estabelecer definições para as terminologias utilizadas nesta pesquisa, partimos do conceito que tecnologia é a reunião de conhecimentos vinculados ao "desenvolvimento e concepção dos instrumentos (artefatos, sistemas, processos e ambientes) criados pelo homem através da história para satisfazer suas necessidades e requerimentos pessoais e coletivos" (VERASZTO, 2009, p. 38), englobando tanto os aspectos culturais de uma sociedade como a economia de um Estado.

O uso das tecnologias e, especialmente, da internet tem aumentado de forma significativa. Através do Internet World Stats, um banco de dados mundial sobre o número de usuários de internet, demonstra-se que, no ano de 2021, 67,9% (sessenta e sete vírgula nove por cento) da população mundial total possuem acesso a internet, ou seja, mais da metade da população mundial possui acesso à uma rede informatizada e globalizada.

Por região, denota-se que a américa latina possui, por sua vez, 80,5% (oitenta vírgula cinco por cento) da sua população classificados como usuários de internet, sendo a região da

---

[19] De acordo com o art. 5º, inciso I, da Lei nº 12.965, de 23 de abril de 2014, a qual estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, considera-se internet "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes".

África a que possui o menor número de usuários que acessam a internet, apenas 43,2% (quarenta e três vírgula dois por cento). Dessas estatísticas podemos ressaltar a importância do estudo sobre tecnologia nas mais diversas áreas, uma vez que o aumento no número de usuários ao longo dos anos sem uma regulamentação que acompanhe esse crescimento pode significar em maiores vulnerabilidades do ponto de vista social, econômico e também criminal.

Gráfico 1 – Estatísticas mundiais de utilização da internet e estimativas da população

WORLD INTERNET USAGE AND POPULATION STATISTICS 2023 Year Estimates						
World Regions	Population (2022 Est.)	Population % of World	Internet Users 31 Dec 2021	Penetration Rate (% Pop.)	Growth 2000-2023	Internet World %
Africa	1,394,588,547	17.6 %	601,940,784	43.2 %	13,233 %	11.2 %
Asia	4,352,169,960	54.9 %	2,916,890,209	67.0 %	2,452 %	54.2 %
Europe	837,472,045	10.6 %	747,214,734	89.2 %	611 %	13.9 %
Latin America / Carib.	664,099,841	8.4 %	534,526,057	80.5 %	2,858 %	9.9 %
North America	372,555,585	4.7 %	347,916,694	93.4 %	222 %	6.5 %
Middle East	268,302,801	3.4 %	206,760,743	77.1 %	6,194 %	3.8 %
Oceania / Australia	43,602,955	0.5 %	30,549,185	70.1 %	301 %	0.6 %
WORLD TOTAL	7,932,791,734	100.0 %	5,385,798,406	67.9 %	1,392 %	100.0 %

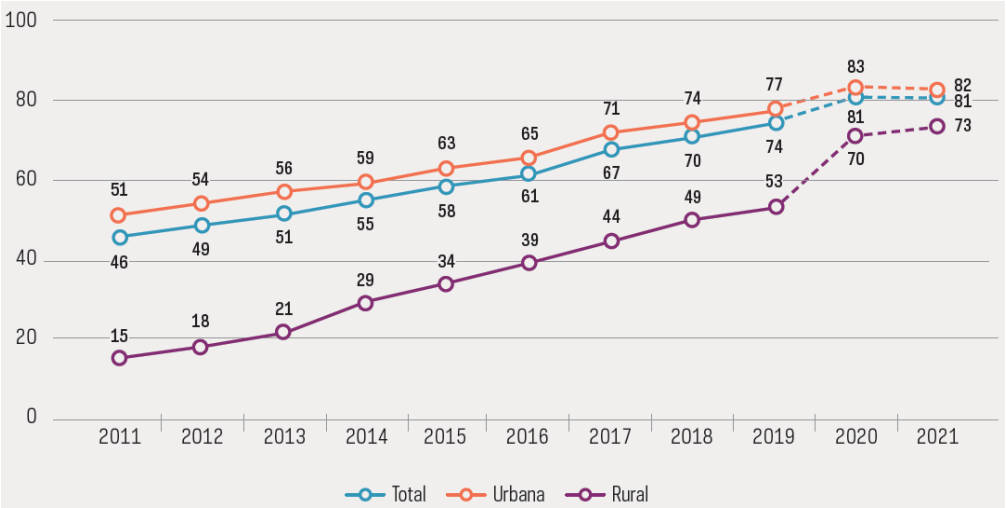
Fonte: Internet World Stats (2023).

Já no âmbito nacional, em pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros do ano de 2021, realizado pelo Comitê Gestor da Internet no Brasil, através da realização de entrevistas presenciais, entre os meses de outubro de 2021 e março de 2022, em 23.950 (vinte e três mil, novecentos e cinquenta) domicílios e com 21.011 (vinte e um mil e onze) indivíduos com 10 (dez) anos ou mais em todo o território nacional, constatou-se que em um intervalo de 10 (dez) anos, de 2011 até o ano de 2021, houve um aumento do número total de usuários de internet de 35% (trinta e cinco por cento).

A pesquisa demonstra que, em 2021, existiam cerca de 59 (cinquenta e nove) milhões de domicílios urbanos com Internet no país, o que equivale a 82% (oitenta e dois por cento) dos domicílios brasileiros. Nos domicílios de áreas rurais, foi possível identificar um crescimento exponencial, já que no ano de 2011 a porcentagem era de apenas 15% (quinze por cento) de usuários com acesso à internet, enquanto em 2021, esse número chegou a 73% (setenta e três por cento), de acordo com o gráfico abaixo.

Gráfico 2 – Usuários de internet por área (2011-2021)

Total da população (%)



Fonte: TIC Domicílios (2021)

Um outro ponto que merece destaque na pesquisa realizada pelo Comitê Gestor da Internet no Brasil está no levantamento de dados sobre as atividades de comunicação, isso porque o Comitê identificou que 93% (noventa e três por cento) dos usuários de internet trocaram mensagens instantâneas, 82% (oitenta e dois por cento) conversaram por chamada de voz ou vídeo e 81% usaram redes sociais. Dessa forma, os dados apresentados pelo Comitê demonstram o crescimento de usuários com acesso à internet nos últimos anos, o que significa uma maior inclusão digital, mas também uma maior necessidade de regulamentação no âmbito da proteção de dados desses indivíduos.

Do ponto de vista do direito criminal, a ausência de normativas específicas e a utilização desmedida dessas informações como prova a ser utilizada na persecução penal vem gerando controvérsias na seara judicial. O Poder Judiciário tem sido provocado para se posicionar sobre a legalidade e permissividade dessas provas. Exemplo disso foi o entendimento da 5ª Turma do Superior Tribunal de Justiça que deu provimento a recurso em *Habeas Corpus* nº 143.169, do Rio de Janeiro, julgado em 25 de outubro de 2022, para anular provas digitais coletadas pela polícia no âmbito da operação *Open Doors*, a qual apurava a existência de uma suposta organização criminosa voltada à prática de furtos eletrônicos contra instituições financeiras.

O caso merece destaque já que durante a coleta do material eletrônico apreendido, a polícia deixou de documentar procedimentos necessários ao manuseio dos computadores apreendidos, o que ensejou a quebra da cadeia de custódia e a consequente inadmissibilidade

das provas em questão. Esse julgado, bem como o tema da cadeia de custódia será tratado de forma mais específica no tópico 3.2, mas é imprescindível nesse momento demonstrar que o Judiciário foi instado a se manifestar sobre procedimentos específicos sobre a coleta de equipamento eletrônicos que não estavam sendo observados pelos agentes policiais, o que revela a premência em se debruçar sobre essa temática.

De acordo com Pinheiro (2021, p. 47), a existência de debates e conflitos sobre matérias que ainda não estão devidamente tratadas em leis mais específicas tem sido o maior desafio para os magistrados, isso porque dá margem para diferentes tipos de interpretação, citando, por exemplo, a dificuldade de se delimitar o direito à liberdade de expressão e o seu abuso que pode acabar ocasionando o crescimento do cometimento de crimes contra a honra, ou a dificuldade na tipificação de algumas condutas e na comprovação da autoria no mundo digital, destacando a forma polêmica de associar endereços de protocolo de internet (endereço IP)[20] a determinada pessoa e vincular a ela uma conduta ilícita, uma vez que esses endereços não estão necessariamente associados a uma pessoa física e deve prevalecer o princípio do *in dubio pro reo*.

Na seara investigativa é possível encontrar ainda mais dificuldades, isso porque os inquéritos policiais ainda são obsoletos quando observada a possibilidade de utilizar a tecnologia como facilitador para as atividades de investigação e repressão de infrações penais. Se considerarmos, por exemplo, os inquéritos instaurados em decorrência de crimes violentos intencionais, os quais a polícia, notadamente, investiga com base apenas em depoimentos de testemunhas, veremos que uma grande parcela desses inquéritos não é concluída de forma resolutiva.

O capítulo *Os inquéritos policiais relativos aos crimes violentos letais intencionais no estado do Rio Grande do Norte e o dilema da ausência de identificação de autoria*, publicado pelos participantes do projeto de pesquisa *Criminalidade violenta, justiça criminal e diretrizes para política de segurança pública do estado do Rio Grande do Norte*, abordou o estudo sobre as decisões de arquivamento, baseados na ausência de autoria, de inquéritos policiais instaurados sobre crimes violentos letais no estado do Rio Grande do Norte entre os anos de 2016 e 2020.

Um dos objetivos da pesquisa foi analisar a relação entre a (in)eficiência das investigações sobre mortes violentas no Rio Grande do Norte e a criminalidade violenta no

[20] Nos termos do art. 5º, inciso III, da Lei nº 12.965/2014, endereço de protocolo de internet é "o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais".

estado para, posteriormente, identificar o que poderia justificar o alto índice de pedidos de arquivamento de inquéritos policiais por ausência de autoria na Polícia Civil do estado do Rio Grande do Norte. A pesquisa foi dividida entre etapas, sendo a primeira a coleta de dados sobre crimes violentos letais intencionais no estado do RN e a segunda etapa ficou responsável pela identificação dos fundamentos dos pedidos de arquivamento dos inquéritos policias relacionados a esses tipos de crime.

Para chegar ao resultado, o grupo, através de base de dados fornecida pelo Observatório de Violência do Rio Grande do Norte (OBVIO), delimitou o total de 223 (duzentos e vinte e três) inquéritos arquivados que visavam a investigação de crimes de homicídio ocorridos entre os anos de 2016 e 2020. A partir desse filtro, foi realizada consulta no sítio eletrônico do Tribunal de Justiça do Rio Grande do Norte com o objetivo de identificar a motivação do arquivamento, o que gerou um número de 20 (vinte) inquéritos policias em tramitação direta entre a polícia civil e o Ministério Público, 44 (quarenta e quatro) não encontrados na plataforma, 30 (trinta) em que não foi possível identificar a razão do arquivamento, uma vez que as sentenças se resumiam a informar ausência de justa causa e/ou condições da ação, restando a quantidade de 129 (cento e vinte e nove) inquéritos arquivados por ausência de identificação da autoria.

Gráfico 3 – Análise dos Inquéritos Policiais arquivados no estado do Rio Grande do Norte

Julgados	02
Mortes com informação de arquivamento da investigação	223
Análise dos IPs nos quais consta a informação de arquivamento	
IPs que na verdade ainda estão tramitando	20
IPs que não foi possível localizar no sítio do TJRN	44
IPs que não foi possível identificar o motivo do arquivamento nasentença	30
IPs arquivados em decorrência da ausência de identificação de autoria	129

Fonte: Política Criminal UFRN (2022)

No entanto, para que fosse possível vincular o índice de arquivamento de inquéritos policiais como justificativa para o baixo nível de efetividade das investigações criminais no estado do Rio Grande do Norte, seria necessário um levantamento de dados oficiais mais condizentes com a realidade, isso porque o próprio projeto de pesquisa faz a ressalva sobre a dificuldade em conseguir ter acesso aos dados oficiais para o estudo (MEDEIROS *et al*., 2022, p. 59).

Nesse contexto, através da pesquisa *Onde mora a impunidade?* realizada pelo Instituto Sou da Paz, e publicada no ano de 2022, o qual visa coletar dados junto aos 26 (vinte e seis) estados brasileiros e ao Distrito Federal com o intuito de estabelecer um indicador nacional de esclarecimentos de homicídios, foi informado que o estado do Rio Grande do Norte, desde a primeira edição do projeto, no ano de 2017, até o ano de 2022, não enviou resposta, informou que não dispõe de dados e/ou os dados são incompletos (INSTITUTO SOU DA PAZ, 2022, p. 14).

Em outra pesquisa, elaborada Associação dos Delegados da Polícias do Brasil (ADEPOL DO BRASIL) a partir de requerimento do Presidente da Comissão de Segurança Pública e Combate ao Crime Organizado da Câmara dos Deputados, o Deputado Emanuel Pinheiro Neto, foi disponibilizado um questionário para todos os estados do Brasil e o Distrito Federal a fim de realizar o levantamento do índice de resolutividade dos inquéritos policiais nas polícias civis de cada ente e da polícia federal.

Acontece que, no mesmo caminho da pesquisa elaborada pela UFRN e pelo Instituto Sou da Paz, ao responder o questionamento sobre a existência de algum índice de resolução de inquéritos policiais em base anual da Polícia Civil e, caso existente, qual seria o indicador de resolutividade considerando a proporção entre inquéritos instaurados e relatados, o estado do Rio Grande do Norte informou que a Polícia Civil do RN não possui dados de resolutividade das delegacias, acrescentando que com a implantação de todos os módulos do Sistema de Informações de Segurança Pública, Prisionais e sobre Drogas – Procedimentos Policias Eletrônicos (SINESP-PPE) essas informações poderão ser extraídas (ADEPOL DO BRASIL, 2022, p. 49).

Por fim, o Anuário Brasileiro de Segurança Pública, publicado no ano de 2022, formado através das informações fornecidas pelas próprias secretarias de segurança pública, pelas polícias civis, militares e federais, entre outras fontes oficiais, também deixou de informar os dados estatísticos referente ao estado do Rio Grande do Norte sobre o volume de ocorrências policiais registradas em relação às mortes que ainda estão pendentes de esclarecimento (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2022, p.142).

Dessa forma, diante das quatro pesquisas aqui mencionadas, constata-se que a ausência de um banco de dados oficial sobre a instauração de inquéritos policiais dificulta a análise precisa sobre a (in)efetividade das investigações criminais, por outro lado, evidencia a falta de estruturação mínima de órgãos policiais estadual para controle e aprimoramento do procedimento investigatório.

Apesar da ausência de fornecimento de dados completos por parte do estado do Rio Grande do Norte, através da pesquisa realizada pela UFRN é possível inferir a grande quantidade de inquéritos policiais que foram arquivados diante da dificuldade em identificar o autor do crime. Esse óbice pode ser facilmente agravado diante da demora no desenvolvimento dessas investigações, isto é, quanto maior o lapso temporal entre a data do fato típico e a conclusão do inquérito, maior é a probabilidade de não conseguir identificar a autoria.

Nesse aspecto, o presente estudo visa analisar se a utilização de procedimentos de investigação assessorados da tecnologia podem viabilizar uma diminuição significativa do número de inquéritos policiais arquivados por ausência de identificação de autoria, mas para isso é necessário compreender o conteúdo relacionado às provas digitais e como funcionaria a sua regulamentação no âmbito jurídico.

3.1 **Conceito e características das provas digitais**

Apesar de existirem controvérsias sobre o sistema seguido pelo processo penal brasileiro contemporâneo, a verdade é que mesmo sendo considerado um sistema acusatório ou misto para alguns doutrinadores[21], uma das suas principais finalidades é a busca pela reconstituição de um fato histórico, ou seja, a análise de um fato típico cometido anteriormente, sendo a prova um elemento imprescindível para essa reconstrução (LOPES JÚNIOR, 2019)[22]. Nesse sentido, Badaró (2021)[23] pontua que proceder a essa reconstrução histórica dos fatos, observados a normativa legal sobre investigação, admissão, produção e a própria valoração dessas provas, é um dos objetivos principais do processo penal.

Carnelutti (2009)[24], em sua obra *As misérias do processo penal*, já relatava a importância e o cuidado que os sujeitos do processo penal devem ter com a produção da prova, isso porque na mesma velocidade em que recai uma suspeita sobre um determinado indivíduo, ele, a sua família, a sua casa, o seu trabalho, são submetidos a inquirições, exames e despidos sem qualquer discrição. Para o autor, essa produção probatória desarrazoada transforma o indivíduo em pedaços, e "o indivíduo, recordemo-nos, é o único valor que deveria ser salvo pela civilidade".

---

[21] Para Aury Lopes Jr. (2019), o sistema processual penal atual não pode ser definido como um sistema acusatório, inquisitório ou misto, isso porque o critério de separação das atividades de acusar e julgar é insuficiente para determinar o sistema atual.

[22] Documento eletrônico não paginado.

[23] Documento eletrônico não paginado.

[24] Documento eletrônico não paginado.

Certo é que a prova é o elemento central do processo penal e, portanto, deve ser compreendida desde a sua terminologia. Capez (2021)[25] esclarece que a palavra prova vem do latim *probatio*, e pode ser considerado o "conjunto de atos praticados pelas partes, pelo juiz (CPP, arts. 156, I e II, 209 e 234) e por terceiros (p. ex. peritos), destinados a levar ao magistrado a convicção acerca da existência ou inexistência de um fato". Logo, a prova seria um instrumento utilizado pelos sujeitos do processo penal para comprovar a veracidade de uma alegação.

Para Badaró (2021), a prova pode ser considerada como o meio pelo qual o magistrado tem possibilidade de chegar à verdade, convencendo-se sobre a ocorrência ou não dos fatos que são juridicamente relevantes para o julgamento do processo. No entanto, é importante esclarecer que não existe reprodução da verdade no processo penal, isso porque a produção de provas durante o procedimento apenas assegura uma maior proximidade com a hipótese dos fatos, auxiliando o magistrado na busca por um conhecimento mais verídico possível, mas não o reflexo de uma "verdade real".

Lopes Júnior (2020, p. 1245), por sua vez, aduz que as provas "são os meios através dos quais se fará essa reconstrução do fato passado (crime). O tema probatório é sempre a afirmação de um fato (passado), não sendo as normas jurídicas, como regra, tema da prova". Assim, partindo da concepção desses três autores e de tantos outros que estudam a temática, é possível compreender prova como um meio a ser utilizado pelas partes do processo penal para comprovar a ocorrência dos fatos históricos em busca de uma maior conformidade com a realidade para auxiliar a apreciação pelo juízo.

No entanto, é importante esclarecer que, apesar das partes do processo penal – acusação e defesa – possuírem o direito de produzir as suas próprias provas, Prado (2014, p. 37) relembra que "em um processo penal regulado pela presunção de inocência, o fato – em realidade, o enunciado sobre o fato – deve ser definido pelo acusador e é este que tem interesse em demonstrar a sua existência", isto é, o ônus da prova recai sob o órgão acusatório, qual seja, o Ministério Público que possui a obrigatoriedade de comprovar inicialmente os fatos pelos quais estará denunciando determinado indivíduo.

Antes de conceituarmos o que seria prova digital, é importante observar que apesar do ônus probatório recair sobre o órgão do Ministério Público, conforme denota-se da leitura da

---

[25] Documento eletrônico não paginado.

própria constituição em seus arts. 129[26] e 144[27], respectivamente, o Código de Processo Penal traz, em seu art. 156, a temática da iniciativa probatória do magistrado.

A redação originária do CPP de 1941 dispunha que "a prova da alegação incumbirá a quem a fizer; mas o juiz poderá, no curso da instrução ou antes de proferir a sentença, determinar, de ofício, diligências para dirimir dúvida sobre ponto relevante", trazendo um nítido caráter inquisitivo oriundo de um contexto político ditatorial e policialesco, cujo propósito era promover um modelo de repressão estatal.

Acontece que, mesmo após a publicação da Lei nº 11.690, de 9 de junho de 2008, o qual foi responsável por alterar alguns dispositivos do Decreto-Lei nº 3.689, de 3 de outubro de 1941 – CPP, a nova redação do art. 156 continuou refletindo o caráter inquisitivo do processo penal, em evidente contradição com o estado democrático de direito atual, uma vez que traz a figura do juiz como sujeito participante da reprodução histórica dos fatos, se afastando de um posicionamento equidistante e imparcial.

Marques (2007, p. 174), por sua vez, aponta que é possível a atividade probatória do juiz, mas esta deve estar "adstrita à tutela da liberdade, sendo-lhe vedado suprir deficiência ou omissão na produção da prova, por parte do Órgão legitimado para promove a acusação", isto é, o magistrado não pode intervir na produção probatória de modo a suprir os erros ou equívocos cometidos pelo Ministério Público, sob pena de estar ultrapassando os limites da sua imparcialidade. Logo, é possível a participação do magistrado na produção de provas, mas essa atividade probatória deve ser realizada observados os limites da Constituição Federal, isso porque deve ser tutelado os direitos fundamentais em detrimento do mito da verdade real.

Retornando à temática da delimitação conceitual da prova digital e suas características, é possível perceber que os meios de prova vêm sendo atualizados constantemente com a evolução da tecnologia. Se antes utilizava-se gravadores, fitas, *pen drives*, CDs ou DVDs, por exemplo, atualmente se discute as provas oriundas da inteligência artificial, *smartphones* e o seus aplicativos como *WhatsApp, Telegram* e até mesmo a utilização de instrumentos que são capazes de controlar o servidor e ocultar determinadas informações.

Nesse sentido, é perceptível que a tecnologia trouxe muitas ferramentas novas para a validação jurídica de uma prova, já que é muito mais provável que haja uma maior força legal

---

[26] Art. 129. São funções institucionais do Ministério Público: [...] VIII - requisitar diligências investigatórias e a instauração de inquérito policial, indicados os fundamentos jurídicos de suas manifestações processuais;

[27] Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: I - polícia federal; II - polícia rodoviária federal; III - polícia ferroviária federal; IV - polícias civis; V - polícias militares e corpos de bombeiros militares; VI - polícias penais federal, estaduais e distrital. [...].

vinculada em uma prova eletrônica, como um e-mail ou mensagens interceptadas, do que uma prova testemunhal ou um fax, o que se aplica também nos casos de assinatura digital ou biométrica em detrimento de anotações em papel sobre o número do Registro Geral (RG) ou do Cadastro de Pessoa Física (CPF) (PINHEIRO, 2021)[28].

Exemplo dessa diferenciação entre as provas mais tradicionais e as provas digitais pode ser encontrada em casos práticos. Imagine a realização do crime de furto realizado através de acesso indevido a uma conta digital bancária. Nesse caso, a vítima encontrará somente a subtração de valores de sua conta bancária, mas dificilmente encontrará sinais da ação criminosa em si. Por outro lado, em um crime de homicídio praticado com arma de fogo, é possível visualizar as lesões no cadáver da vítima ou em um furto qualificado por rompimento de obstáculos, os danos na porta de acesso. Esses exemplos apenas demonstram que os crimes praticados pelos meios informáticos apesar de deixarem mais elementos de novos para comprovar a ação criminosa, o fato de não serem corpóreos ou materiais demandam um estudo mais específico (KIST, 2019, p. 106).

Levando em consideração premissas e peculiaridades que envolvem esse tipo de prova, Vaz (2012, p. 63), define prova digital como os dados em forma digital, os quais podem conter determinada representação de fatos ou ideias, encontrados em um suporte eletrônico ou transmitidos em rede de comunicação. A autora exclui dessa definição tanto os meios de prova – como simulações elaboradas no computador ou reconstituições de fatos em programas informáticos – bem como as informações registradas em meios digitais que possam ser obtidas de entidades públicas ou terceiros através de requisição. Para ela, somente seriam provas digitais aquelas oriundas de meios de obtenção como buscas e apreensões, interceptações ou acessos em redes ou servidores, por exemplo.

Para Kist (2019, p. 107), a prova digital é aquela derivada de dispositivos informáticos, por meio dos quais podem processar e transmitir informações e dados. O autor também toma o cuidado em diferenciar prova eletrônica da prova digital, isso porque apesar daquela ser gênero e esta ser espécie, a prova eletrônica engloba qualquer dispositivo eletrônico, inclusive os analógicos, como eram as gravações de vídeo e áudio realizadas em fitas-rolo e os filmes fotográficos que precisavam ser revelados, enquanto a prova digital é produzida e processada através de um sistema de numeração utilizados na programação da linguagem computacional, independentemente do local que se encontre armazenado (KIST, 2019, p. 107-109).

---

[28] Documento eletrônico não paginado.

Na doutrina estrangeira, Eoghan Casey (2011, p.7), define prova digital ou *digital evidence* como "any data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator[29]", ou seja, a prova digital pode ser considerada como qualquer dado que possa estabelecer que um determinado crime foi cometido ou que comprove o vínculo entre o crime e a vítima ou o autor. Na mesma obra, o autor cita o grupo de trabalho sobre evidência digital[30], criado em 1998, com o objetivo de reunir organizações empenhadas em estudar sobre o campo da evidência digital e promover a comunicação e cooperação, bem como assegurar a qualidade e a coerência na comunidade forense, define prova digital como informação de valor de probatório que é armazenada ou transmitida pela rede de computadores[31] (CASEY, 2011, p. 7).

Assim, prova digital pode ser definida como aquela produzida em formato digital que pode ser armazenada ou transmitida através de sistemas, redes ou equipamentos eletrônicos. As suas características também podem ser percebidas da sua própria definição que denota pontos específicos no que diz respeito ao seu registro, manutenção e extração.

As evidências constituídas a partir de um fato típico na seara digital possuem características específicas quando comparadas com provas físicas provenientes do cometimento de crimes "tradicionais", como é o caso de homicídio, roubo, furto etc. Essas evidências que futuramente podem formar a prova digital a ser utilizada em um processo penal demandam meios de investigação próprios e especificidades para o cumprimento da sua cadeia de custódia, de forma que as suas características devem estar manifestamente definidas para um melhor aproveitamento dessa prova.

A primeira característica percebida por Kist (2019, p. 118) é baseada na imaterialidade ou invisibilidade, já que a prova digital é "composta por uma sequência de *bits*, e existe independentemente do suporte físico no qual é incorporada", ou seja, caso se proceda à abertura de um computador, por exemplo, no seu interior não haverá nenhum documento que possa ser fisicamente apreensível. Outra característica destacada pelo autor se refere à volatilidade e fragilidade, já que o fato da prova digital não precisa de suporte físico para existir, ela pode ser manipulada, perdendo suas propriedades ou até mesmo desaparecendo. Essa segunda característica demanda uma abordagem ainda mais técnica na cadeia de custódia, uma vez que se deve observar rigorosamente a metodologia específica para a sua coleta, sob pena de

---

[29] "Quaisquer dados que possam estabelecer que um crime foi cometido ou que possam fornecer uma ligação entre um crime e sua vítima ou um crime e seu autor" (tradução nossa).

[30] Na versão original, Standard Working Group on Digital Evidente (SWGDE).

[31] Na versão original, "digital evidence in an information of probative value that is stored or transmitted in binary form" (CASEY, 2011, p. 7).

alteração ou perda dos dados. Por fim, a terceira característica da prova digital para Kist consiste na sua maior probabilidade de dispersão, na medida em que a prova pode estar localizada em diversos locais diferentes, seja dentro do próprio sistema informático ou em locais geográficos diferentes (KIST, 2019, p. 120).

Para Denise Vaz (2012, p. 67), por sua vez, a prova digital possui como características a (i) imaterialidade e desprendimento do suporte físico originário, (ii) volatilidade, (iii) suscetibilidade de clonagem e (iv) necessidade de intermediação de equipamento para ser acessada. Para a autora, a (i) imaterialidade corresponde ao fato de que os dados digitais são impalpáveis já que consistem em impulsos elétricos que podem ser armazenados em grande quantidade e transferidos a outros dispositivos eletrônicos, sem ocupar espaço físico relevante e sem perder a sua essência.

A (ii) volatilidade seria a fragilidade da prova digital, isso porque pode ser facilmente submetida a alterações ou o desaparecimento, de modo a se tornar uma prova frágil diante das manipulações que podem prejudicar a sua confiabilidade. A terceira característica, por sua vez, decorre da facilidade em executar infinitas cópias sem conseguir determinar qual seria o exemplar original. Por fim, a (iv) necessidade de intermediação significa a exigência de determinado equipamento que possa processar a informação buscada na investigação e disponibilizá-la de uma forma acessível ao ser humano, já que os dados digitais são formados por sequenciais numéricos, muitas vezes codificados (VAZ, 2012, p. 67).

Desse modo, denota-se que as características das provas digitais podem ser resumidas na imaterialidade, fragilidade e dispersão, fazendo com que os órgãos de investigação e acusação – Ministério Público e órgãos policiais – precisem além de investimento nas áreas de tecnologia para facilitar a apreensão de materiais digitais, capacitação dos seus servidores e agentes para identificar e coletar de forma diligente provas que podem ser modificadas ou desaparecer em questão de minutos.

Prova dessas características podem ser facilmente encontradas em casos reais ocorridos recentemente, como os chamados ciberataques vinculados à Rússia. Apesar da divulgação de informações em diversas plataformas jornalísticas associando a responsabilidade do país russo à ataques cibernéticos nos mais diversos países – inclusive durante a campanha presidencial dos Estados Unidos da América (EUA) em 2016, ainda não foi possível identificar o local específico em que foi utilizado o programa para o planejamento e desenvolvimento desses ataques, fazendo com que se torna cada vez mais difícil a coleta dessa prova digital.

Outro exemplo emblemático foi o caso da Microsoft Irlanda. Em resumo, esse caso diz respeito a um pedido de busca e apreensão realizado pelo Poder Judiciário dos Estados

Unidos com o objetivo de coletar informações de uma conta de e-mail mantida e controlada pela empresa Microsoft. Acontece que houve resistência por parte da empresa na entrega desse conteúdo, uma vez que apesar do controle estar adstrito à empresa situada nos Estados Unidos, a informação, isto é, os dados de conteúdo estavam armazenados pela empresa situada na República da Irlanda, o que, na visão da empresa, demandaria um pedido formal de cooperação internacional, sem a possibilidade de um acesso direto (DE ABREU, 2017, p. 109).

O caso da Rússia e da Microsoft Irlanda retratam, portanto, a problemática por trás das características das provas digitais. A imaterialidade, volatilidade e a dispersão, destacada por Kist (2019), revelam a urgência em se discutir sobre a obtenção dessas provas digitais para que sejam, de fato, utilizadas devidamente na persecução penal. Os casos concretos demonstrados anteriormente revelam a morosidade em conseguir ter acesso à essas provas, seja por encontrar barreiras na legislação aplicável ou pela dificuldade em localizar geograficamente o local onde esses dados são armazenados.

Acontece que para a compreensão da prova digital e o regime jurídico adequado a ser aplicado por esses órgãos, faz-se necessário distinguir também os dados resultantes dos serviços de telecomunicações que servirão de parâmetro para os próximos tópicos. Kist (2019, p. 110-111) destaca que podem ser analisados dados de base, dados de tráfego e dados de conteúdo.

Os dados de base, também conhecidos como dados cadastrais no Brasil, são aquelas informações sobre nome, números de registro geral e cadastro de pessoas físicas, endereços, telefones etc., fornecidas voluntariamente em rede de comunicações eletrônicas.

Os dados de tráfego são aqueles que surgem da transmissão de mensagens pela rede, podendo demonstrar tempo, duração, formato de envio de mensagem e também a localização geográfica do equipamento utilizado pelo emitente e destinatário. Esse tipo de dado foi definido pela própria Convenção de Budapeste, em seu art. 1º, e designa “quaisquer dados de computador referentes a uma comunicação por meio de um sistema informatizado, gerados por um computador que seja parte na cadeia de comunicação”, indicando, conforme já explicitado, a origem, destino, caminho, hora, data, extensão, duração ou tipo de serviço subordinado.

Por fim, os dados de conteúdo são as próprias mensagens transmitidas, isto é, a mensagem propriamente dita. O Relatório Explicativo da Convenção de Budapeste esclarece, em seu ponto 209, que o termo dados de conteúdo não foi definido ao longo da Convenção, mas se refere ao “conteúdo informativo da comunicação, ou seja, o significado ou o teor da comunicação, ou a mensagem ou informação veiculada pela comunicação (que não a relativa aos dados de tráfego)”. Desse modo, definidos os conceitos necessários que envolvem a

temática da prova digital, se faz necessário analisar a sua produção probatória e os meios de obtenção utilizados pelas autoridades competentes.

3.2 **Produção e os meios de obtenção da prova digital**

As provas digitais coletadas no interesse da persecução penal podem ser encontradas tanto em um dispositivo eletrônico, como também podem estar em movimento de tráfego por uma rede, especialmente a internet, de modo que a sua coleta será basicamente através de um suporte físico ou através da coleta apenas dos dados digitais. Nesse sentido, a prova poderá ser apresentada em juízo basicamente de duas formas: como uma prova documental, no caso de o documento ser retirado do suporte físico, ou como uma prova pericial, se demandar conhecimentos técnicos específicos para a sua extração (VAZ, 2012, p. 81).

Até pouco tempo não existia na legislação brasileira um regramento específico sobre os meios de obtenção de provas digitais, sendo a coleta desses dados digitais adaptados aos três meios mais conhecidos no contexto brasileiro: (i) busca e apreensão, (ii) interceptações telefônicas e, ainda o (iii) acesso remoto a redes e serviços, este último passível de discussão no âmbito doutrinário.

A busca e apreensão, como meio de obtenção de prova, sempre foi regulamentada ao longo da história processual. Acontece que a elaboração do Código de Processo Penal de 1941, em um contexto político extremamente opressor, influenciou na elaboração dos arts. 240 a 250 do CPP, fazendo com que diversas terminologias adotadas pelo legislador sofressem com a ausência de uma interpretação exata. Exemplo dessa temática foram os conceitos de *fundadas razões* ou até mesmo *fundada suspeita* que deixaram margem à discricionariedade da autoridade competente.

Outra problemática identificada na utilização da medida de busca e apreensão foi o fato de que o legislador assegurou tanto à autoridade policial, como à judiciária, a competência para a execução dessa medida, independentemente de mandado judicial (CORTEZ, 2023). Nesse ponto, é necessário analisar a legislação infraconstitucional através de atual contexto constitucional e garantista, o que faz com que seja possível reduzir eventuais danos de uma legislação que sequer passou pelo crivo do Congresso Nacional na época em que foi elaborada. No que se refere à temática das provas digitais, percebe-se um detalhe interessante sobre a utilização da ordem terminológica, uma vez que no que se refere às provas imateriais, primeiro o agente competente deverá apreender o dispositivo eletrônico utilizado para depois proceder a busca, algo diverso do que acontece normalmente com as provas materiais.

As interceptações telefônicas, por sua vez, foram regulamentadas a partir da Lei nº 9.296, de 24 de julho de 1996, a qual assegura que esse meio de obtenção de prova somente poderá ser utilizado se houver indícios razoáveis de autoria ou participação na infração penal, se a prova não puder ser feita por outros meios disponíveis e prevê, ainda, a proibição de sua utilização nos casos de a infração penal investigada ser punido, no máximo, com pena de detenção, restringindo a sua aplicação na seara criminal. Para fins de autorização, a lei determina que somente a autoridade judicial, de ofício ou através de requerimento da autoridade policial, na investigação criminal, ou do representante do Ministério Público, na investigação criminal e na instrução processual penal, poderá emitir essa ordem, de modo que as interceptações telefônicas realizadas sem autorização judicial poderão ser consideras ilícitas.

Observa-se, mais uma vez, a flexibilização dos direitos fundamentais resguardados pela Constituição Federal de 1988, uma vez que a garantia de inviolabilidade da intimidade não pode servir como um "escudo protetivo da prática de atividade ilícitas, nem tampouco como argumento para afastamento ou diminuição da responsabilidade civil ou penal por atos criminosos" (PINTO, 2017, p. 62).

O sigilo das comunicações telefônicas, garantido pelo inciso XII do art. 5º da Constituição Federal merece uma atenção especial ao presente estudo, isso porque o constituinte optou por mencionar no final do inciso apenas a terminologia *comunicações telefônicas*. Essa discussão foi objeto de estudo de diversos doutrinadores, chegando à conclusão de que a previsão exposta pelo legislador no parágrafo único do art. 1º da Lei das Interceptações Telefônicas era constitucional. O legislador, preocupado com a abrangência da norma, expôs que a interceptação também se aplicaria às comunicações realizadas em sistemas de informática e telemática, fazendo com que as transmissões eletrônicas realizadas pela internet, através de uma combinação do uso do computador e dos meios de telecomunicações, fossem passíveis de serem interceptadas (SILVA JÚNIOR, 2021, p. 504).

Nesse sentido, Silva Júnior (2021, p. 504) abordou o avanço da tecnologia e a possibilidade de transmissão e recepção de mensagens, áudios e imagens através do serviço de internet prestado por empresas de televisão a cabo, de modo que a comunicação antes realizada por sistema de telecomunicações deixasse de ser a única opção ao usuário.

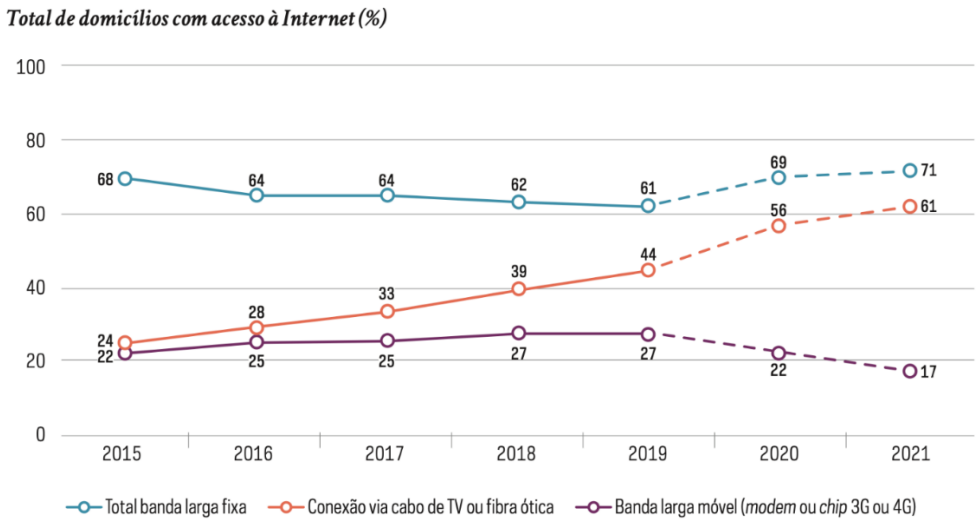
Atualmente, já é possível avançar a discussão e a aplicabilidade da lei para serviços de internet via satélite. Essa forma de acesso à internet tem sido desenvolvida por grandes empresas para facilitar a sua utilização, principalmente para as pessoas que vivem em regiões mais afastadas dos centros urbanos, sem opções de conexão. Esse tipo de conexão utiliza satélites localizados na órbita terrestre que possibilita o envio e retorno de dados através de um

modem e uma antena instalados pelo usuário (DA SILVA OLIVEIRA *et al*., 2022, p. 3), logo, sem a necessidade de serviços de telefonia ou de cabos.

Dessa forma, a internet via satélite é mais um avanço da tecnologia que não foi prevista pelo legislador e nem pelo constituinte, o que faz com que novas discussões sobre a legalidade da utilização das interceptações telefônicas nesses casos seja tema do poder judiciário futuramente, já que não se pode falar que se trata de comunicação telefônica.

Acontece que essa, ainda, não é uma realidade tão comum no Brasil. Prova disso foram os dados da pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros (TIC Domicílios 2021), referente ao ano de 2021, o qual demonstrou que o principal tipo de conexão utilizado para acessar a internet nos domicílios é a banda larga, presente em 71% (setenta e um por cento) dos domicílios com acesso à rede no país, número superior ao observado no ano de 2019 (61%). A pesquisa esclarece que esse aumento se deu em razão do avanço da fibra óptica no país, com o aumento da proporção de provedores que foram capazes de ofertar essa tecnologia, inclusive em pequenos municípios.

Gráfico 4 – Domicílios com banda larga fixa, por principal tipo de conexão (2015-2021)



Fonte: Pesquisa TIC Domicílios (2021).

O aumento do número de domicílios com acesso à internet através da utilização de conexão via cabo de TV ou fibra óptica também impactou diretamente na diminuição da utilização de banda larga móvel (*modem* ou *chip* 3G ou 4G), justificado especialmente pelo custo da conexão e pela possibilidade de utilização de Wi-Fi nos domicílios (TIC DOMICÍLIOS, 2021, p. 64).

Por fim, o acesso remoto a redes e serviços gera uma discussão ainda sem solução no âmbito processual penal brasileiro, isso porque ao mesmo tempo em que o interesse estatal cresce acerca do uso de meios digitais para auxiliar na prevenção e repressão de delitos tem aumentado gradativamente, é nítida a falta de instrumento e capacitação para a coleta dessas provas.

Nesse sentido, em pesquisa publicada no livro *Política criminal: monitoramento de espaços públicos, (in) eficiência dos inquéritos policiais, duração razoável dos processos e tratamento dos presos*, foi abordado, especificamente no capítulo 1, a implementação de sistema de videomonitoramento no entorno da sede da Justiça Federal do Rio Grande do Norte (JFRN). O objetivo desse estudo foi verificar a importância da destinação de verbas pela administração pública na área da segurança, bem como analisar a utilização dessa tecnologia para elucidação de crimes durante investigações criminais e ações judiciais (REINALDO; SILVA JÚNIOR, 2022, p. 21-22).

Constatou-se que o sistema de videomonitoramento, apesar de não implicar uma redução significativa no número de delitos, pode ser caracterizado como elemento indispensável para elucidação de crimes, de modo que os investimentos realizados pela administração pública se justificam pela capacidade no desfecho em ações judiciais. Outro ponto levantado pelos autores foi a possibilidade de utilização dessa tecnologia como prova, independentemente de autorização judicial e desde que observados os elementos da cadeia de custódia, uma vez que não interferem nas esferas do direito à privacidade dos cidadãos judiciais (REINALDO; SILVA JÚNIOR, 2022, p. 38).

Outro caso que pode ser analisado na presente dissertação são os *malwares*, os quais podem ser conceituados como um "conjunto específico de *softwares* que, instalados de modo oculto em um equipamento ou sistema informático, permitem a um terceiro não usuário o acesso às informações e dados nele contidos" (RIBEIRO *et al*., 2022, p. 1465). Aury Lopes Júnior (2021) pontua que apesar de alguns países, como a Espanha, Itália e Estados Unidos, já utilizarem essa metodologia para fins investigativos, são diversas as polêmicas encontradas, isso porque por mais que o poder estatal se mostre sutil na utilização dessa tecnologia, as fronteiras de proteção acabam sendo rompidas durante a persecução, fazendo com que seja necessário o "(re)estabelecimento de (novos) limites para preservar garantias individuais".

Fácil é, portanto, imaginar as fronteiras dos direitos à intimidade, privacidade e ao sigilo serem ultrapassadas, sem qualquer norma que assegure os limites dessa intervenção estatal no âmbito privado do indivíduo. O acesso remoto a dados pessoais, a informações profissionais e até mesmo a localização geográfica, sem qualquer fundamentação concreta e

proteção, pode violar as garantias mais básicas do ser humano e transformar em realidade o que foi retratado no clássico livro *1984*, de George Orwell.

Nesse sentido, questiona-se: é lícita a investigação criminal a partir da utilização de *malwares*? A resposta deve ser embasada de forma muito objetiva. Um dos principais princípios que norteiam o direito brasileiro é a legalidade, isto é, para aplicação de instrumentos, como meios de obtenção de prova, faz-se necessário a sua previsão em lei. Denota-se que a busca e apreensão e a interceptação de comunicações telefônicas estão previstas em leis vigentes, o que é não é o caso do acesso remoto à rede e serviços através de *softwares* instalados de modo oculto.

Ribeiro *et al*. (2022, p. 1495) aponta que não é possível sustentar a existência de uma previsão legal a partir das Leis nº 9.296, de 24 de julho de 1996 (Lei das interceptações telefônicas), 12.850, de 2 de agosto de 2013 (Lei que define organização criminosa e dispõe sobre meios de obtenção de prova) e a 8.069, de 13 de julho de 1990 (Lei que dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências). A primeira já foi citada nesse estudo e em nada se confunde com o acesso remoto a redes e serviços de terceiros, já que trata especialmente da interceptação de comunicação de dados. As duas últimas leis foram citadas pelos autores por preverem ao longo do seu texto a possibilidade de infiltração de agentes policiais na investigação de determinados crimes, mas que também não tratam sobre o emprego de dispositivos espiões em atividades daquela natureza.

Conforme mencionado anteriormente, o ordenamento jurídico brasileiro até pouco tempo não contemplava normas específicas sobre a obtenção e produção da prova digital, o que fazia com que discussões sobre o uso de analogia para o procedimento probatório ou a proibição do método probatório fossem temáticas levantadas pelos doutrinadores e pelo poder judiciário (VAZ, 2012, p. 80). Contudo, no dia 12 de abril de 2023, foi publicado o Decreto nº 11.491, o qual promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.

No que se refere aos meios de obtenção de provas digitais, a Convenção de Budapeste apresenta, basicamente, seis formas, quais sejam: (i) a preservação expedita de dados de computador, (ii) a preservação expedita e revelação parcial de dados de tráfego, (iii) ordem de exibição, (iv) busca e apreensão de dados de computador, (v) a obtenção de dados de tráfego em tempo real e (vi) a interceptação de dados de conteúdo.

De acordo com o art. 16 da Convenção de Budapeste, o primeiro meio de obtenção de provas digitais tem como objetivo a conservação de dados de computador para posterior utilização na persecução penal, uma vez que são mais suscetíveis à perda ou alteração (MINTO,

2021, p. 37). A Convenção dispõe ainda que o Estado deverá preservar e manter a integridade desses dados pelo período de tempo necessário, sem ultrapassar o tempo máximo de 90 (noventa) dias, podendo ser prevista a subsequente renovação da ordem (art. 16, nº 2).

Essa limitação temporal para o armazenamento dos dados digitais coletados, bem como a manutenção do sigilo por parte do detentor dos dados ou terceiro encarregado (art. 16, nº3), demonstra a preocupação do legislador internacional sobre o controle e a segurança desse armazenamento para fins de persecução penal, isso porque são inúmeros os exemplos de compartilhamento de informações sigilosas, em evidente violação ao determinado pela lei.

No âmbito nacional, o Conselho Nacional de Justiça publicou a Resolução nº 217, de 16 de fevereiro de 2016, passando a estabelecer a obrigatoriedade dos magistrados em determinar a instauração de investigação sempre que houver vazamento seletivo e ilegal de dados e informações sigilosas constantes de procedimentos investigatórios. Um dos fatores para normatização dessa medida foi a normalização da exposição midiática que estava ocorrendo com o vazamento de informações relacionadas à acordos de colaboração premiada, interceptações telefônicas e documentos apreendidos em grandes operações.

A preservação expedita e revelação parcial de dados de tráfego, previsto no art. 17, da Convenção de Budapeste, prevê, por sua vez, a identificação dos provedores de serviço e o caminho por meio do qual a comunicação se realizou, devendo ser observada todo o regramento previsto no artigo anterior para a sua preservação e manutenção.

Kist (2019, p. 140) esclarece que a importância da preservação desses dados digitais se dá pelo fato de que os crimes cometidos com o auxílio de meios informáticos e tecnológicos, principalmente através da transmissão de comunicações, estão sujeitos a ingerências que as alteram ou as eliminam, fazendo com que as provas essenciais à persecução penal sejam perdidas. Desse modo, o autor expõe que “a medida de preservação de dados é expediente essencial na investigação desta criminalidade e na resposta estatal às ações dos criminosos de ocultarem a sua atividade ilícita”.

O terceiro meio de obtenção de prova é a ordem de exibição (art. 18), a qual é dirigida a qualquer pessoa ou provedor de serviço para que apresente os dados de computador especificados ou as informações cadastrais necessárias às autoridades competentes. Nessa acepção, a medida é uma alternativa menos intrusiva quando comparada à busca e apreensão de dados informáticos, já que concede às instâncias investigatórias a possibilidade de obrigar uma pessoa a fornecer os dados armazenados em seu poder, e aos fornecedores de serviços a prestarem informações sobre os seus clientes (KIST, 2019, p. 146).

Esse ponto merece uma ressalva quanto à recusa da ordem de exibição, isso porque há determinadas matérias que são passíveis de sigilo, como é o caso do sigilo profissional do médico ou advogado, o sigilo fiscal ou bancário. No entanto, como foi esclarecido no início do estudo, não há direito fundamental absoluto, logo, na medida em que for comprovada e justificada a necessidade de quebra desse sigilo por parte da autoridade competente, torna-se possível a flexibilização desses direitos.

No que se refere à busca e apreensão de dados de computador (art. 19), a Convenção não estabelece diferença entre a busca efetuada em suportes físicos ou aquelas realizadas de forma remota (VAZ, 2012, p. 82). De acordo com a disposição da Convenção, os Estados signatários adotarão medidas legislativas para conceder poderes a suas autoridades competentes para busca ou investigação "a. de qualquer sistema de computador ou de parte dele e dos dados nele armazenados" e "b. de qualquer meio de armazenamento de dados de computador no qual possam estar armazenados os dados procurados em seu território".

Para tanto, a autoridade deve demonstrar as fundadas razões para supor que os dados procurados estão armazenados no sistema, e que tais dados são legalmente acessíveis, podendo apreender ou proteger um sistema de computador, fazer cópias, manter a integridade dos dados de computador relevantes, além de tornar inacessíveis os dados acessados no sistema de computador ou dele removê-los.

Apesar da Convenção de Budapeste tratar sobre a busca e apreensão de dados de computador, trazendo uma maior abrangência à sua aplicabilidade nos mais variados sistemas de computador ou aos meios de armazenado, não tratou sobre apreensão de dados relacionados à vida particular do investigado ou de terceiros, o que se convencionou denominar de *dados sensíveis*. Kist (2019, p. 164) aponta que, ao contrário da Convenção, a legislação portuguesa percebeu a relevância desse tema e previu, em seu art. 16, nº3[32], que diante da apreensão de dados dessa natureza, deve a autoridade apresenta-los ao magistrado que possui competência para tomar conhecimento e ponderar sobre a razoabilidade de serem usamos como prova processual penal.

Percebe-se que o legislador português não retirou, de forma automática, a possibilidade de utilização de dados relacionados à vida privada e a intimidade das pessoas atingidas na persecução penal, mas deixou, a critério da autoridade judiciária competente,

[32] Art. 16, nº 3: caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.

afirmar a necessidade desses dados para o processo. Essa ponderação deve ser realizada de forma cautelosa, uma vez que se faz necessário restringir o acesso a esses dados pessoais, além de zelar pelo seu sigilo e armazenamento, sob pena de expor indevidamente e de forma desproporcional aspectos da vida privada de pessoas investigadas ou até mesmo de terceiros não envolvidos.

O título 5 da Convenção de Budapeste traz em seus arts. 20 e 21 as últimas duas formas de obtenção de prova digital, a obtenção de dados de tráfego em tempo real e a interceptação de dados de conteúdo. Importante destacar que o título traz a terminologia *em tempo real*, diferenciando do meio de obtenção da busca e apreensão, uma vez que aqui o legislador quis abordar a coleta de provas de forma concomitante à sua produção, algo similar à interceptação de comunicações telefônicas tratadas pelo legislador brasileiro.

No entanto, ao contrário da legislação brasileira, o Relatório Explicativo da Convenção de Budapeste esclareceu, no ponto 206, a abrangência das interceptações, zelando pela sua aplicabilidade diante do avanço da tecnologia. Afirmou que "a definição de "sistema informático" constante do Art. 1º não limita a forma segundo a qual os dispositivos ou o grupo de dispositivos devem estar interligados", isto é, apesar da interceptação de telecomunicações se referir, normalmente, às redes de telecomunicações tradicionais, nos dias de hoje, as comunicações móveis também se encontram facilitadas por redes de satélite especiais, logo, a convergência das tecnologias de informação e das telecomunicações torna difícil a sua distinção, de modo que o Relatório esclarece que essa forma de obtenção de dados é capaz de englobar qualquer sistema.

O Relatório também aponta que o título 5 da Convenção aborda dois tipos de dados passíveis de serem recolhidos, os dados de tráfego e os dados de conteúdo, definidos no tópico anterior. Relativamente à obtenção de dados de tráfego em tempo real (art. 20), a Convenção possibilita às autoridades competentes a coleta, reunião ou gravação desses dados por meios técnicos, a obrigar um provedor de serviço, nos limites de sua capacidade técnica, e a cooperação com as autoridades competentes ou prestação de auxílio na obtenção ou gravação desses dados.

Um ponto importante dessa forma de obtenção de prova digital é que, em muitos casos, o autor do crime, utilizando-se da tecnologia, adote providências para apagar eventual caminho percorrido por ele para o cometimento do delito, evitando, dessa forma, a apreensão posterior de dados ou documentos. Nesse sentido, é que a Convenção previu a possibilidade de recolha em tempo real dos dados de tráfego, como uma técnica de investigação de extrema importância, a qual permite identificar origem ou destino da mensagem (números de telefone, e-mail, IP etc.)

e dados conexos, como hora, data, duração e até mesmo localização, sobre vários tipos de comunicações ilegais ou comunicações que forneçam informações sobre a existência sobre crimes cometidos anteriormente ou planejamentos futuros.

Contudo, destaca-se a necessidade de ter a recolha de dados de tráfego associado a uma comunicação específica, isto é, a Convenção não autoriza a vigilância ou a recolha de dados de tráfego de forma geral ou indiscriminada. Do mesmo modo, no ponto 219 do Relatório Explicativo também é mencionado a proibição de *missões de exploração*, através das quais se espera descobrir evidências relacionadas a atividades ilegais, sendo esta atividade completamente diferente dos objetivos de uma investigação criminal. Por esta razão, é imprescindível ordem judicial ou autorização da autoridade competente, para que se dê início à obtenção de dados de tráfego em tempo real.

Dentro desses limites, encontra-se a prática de *fishing expedition*, também conhecida como pesca predatória, que é caracterizada pela "investigação especulativa e indiscriminada, sem objetivo certo ou declarado" (SILVA JÚNIOR, 2021, p. 345). Nas palavras do Ministro Gilmar Mendes, no julgamento do Habeas Corpus nº 163.461/PR, *fishing expedition* é uma "investigação genérica para buscar elementos incriminatórios aleatoriamente, sem qualquer embasamento prévio". Tal prática é revelada a partir da utilização de meios de obtenção de prova sem autorização judicial necessária, seja em endereço diverso do que consta no mandado de busca e apreensão ou até mesmo quando os agentes excedem o que foi autorizada pelo magistrado.

De modo diferente, é o encontro fortuito de provas, isso porque a prova da infração legal é encontrada a partir da busca regularmente autorizada para a investigação de outro crime (PACELLI, 2017)[33]. Quando, por exemplo, em uma investigação criminal sobre uma organização criminosa e o suposto cometimento de crime de tráfico de drogas, realizam uma interceptação ou utilizavam como meio de obtenção de prova a coleta de dados de tráfego em tempo real, espera-se que sejam encontradas apenas provas relacionadas aos crimes ali investigados. No entanto, algumas vezes, é possível que sejam encontradas outras provas relacionadas a crimes diversos (por exemplo, crimes de homicídio), de forma que o poder judiciário já decidiu diversas vezes sobre a licitude da prova encontrada de modo fortuito, desde que guarde relação de conexão ou continência com o crime originalmente investigado.

O julgamento paradigma se deu com a decisão do Supremo Tribunal Federal, nos autos do Habeas Corpus nº 83.515/RS, de relatoria do Ministro Nelson Jobim, julgado no ano de

---

[33] Documento eletrônico não paginado.

2004, que ao analisar pedido da defesa sobre a nulidade das provas encontradas fortuitamente por se tratarem de crimes puníveis com detenção e, portanto, impossível de servir como justificativa para autorização da interceptação, decidiu que essas provas por terem sido encontradas de maneira fortuita no âmbito de uma investigação legítima, já que foi iniciada por suspeita de cometimento de crimes punidos com reclusão, seriam consideradas lícitas para a persecução penal.

O relator Ministro Nelson Jobim explica que não seria possível ignorar a presença da prova de crimes que tenham conexão com os orginalmente investigados, já que tratam de crimes cometidos a partir de iguais práticas ou ainda de delitos que englobam o outro. Caso contrário, destaca que "nunca seria possível a interceptação telefônica para a investigação de crimes apenas com reclusão quando forem estes conexos com crimes punidos com detenção". Nesse mesmo sentido, Pacelli (2017)[34] afirma que a impossibilidade de utilização de provas que guardem conexão com o fato original poderia significar um instrumento de "salvaguarda de atividades criminosas", especialmente na sera da criminalidade macroeconômica e das organizações criminosas.

Por último, temos a interceptação de dados de conteúdo (art. 21), em que a Convenção possibilitou aos Estados signatários adotarem as medidas legislativas necessárias para que as autoridades competentes possam, em tempo real, coletar ou gravar tais comunicações ou compelir um provedor de serviço, nos limites de sua capacidade técnica para coletar ou gravar as comunicações, ou cooperar com as autoridades competentes, ou auxiliá-las, na obtenção ou gravação do conteúdo dessas comunicações.

O Relatório Explicativo da Convenção de Budapeste ressalta a importância da recolha de dados relativamente ao conteúdo das comunicações informáticas, justamente pelo fato da tecnologia permitir uma maior transmissão de dados, incluindo textos, imagens e sons, de modo a facilitar a prática de crimes, especialmente que envolvam a distribuição de conteúdos ilegais como, por exemplo, o crime de divulgação de cena de estuprou ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia (art. 218-C, do Código Penal brasileiro).

A interceptação de dados de conteúdo é similar à interceptação das comunicações telefônicas, tratadas anteriormente, mas consegue abordar outros meios de comunicação que antes eram objetos de discussão. Fato é que os sistemas informáticos atuais permitem uma maior conexão entre autores dos crimes, com o objetivo de lograr êxito em um maior número de infrações penais. A interceptação também se justifica como um meio de obtenção de prova

---

[34] Documento eletrônico não paginado.

mais eficiente, quando comparado com a busca e apreensão, na medida em que a supressão dessa prova digital ocorre com maior facilidade. Logo, nas palavras de Kist (2019, p. 183), "é este o contexto em que a obtenção de dados informáticos em tempo real, no exato momento em que são gerados ou transmitidos, é mecanismo eficiente para a investigação da cibercriminalidade".

3.3 **Aspectos relevantes sobre a cadeia de custódia**

Um dos aspectos mais importantes na atividade probatória é a preservação da idoneidade de um trabalho investigativo minucioso e delicado ao longo da persecução penal, com o objetivo de evitar a quebra da cadeia de custódia (*break in the chain of custody*) (PRADO, 2014, p. 77). No entanto, as regras pertinentes à cadeia de custódia somente foram incluídas no Código de Processo Penal brasileiro no ano de 2019, através da Lei nº 13.964, de 24 de dezembro de 2019, conhecida como Pacote Anticrime.

O novo art. 158-A, do CPP, tratou de conceituar cadeia de custódia como o "conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte". Apesar da inovação do legislador em dispor sobre o conceito normativo do instrumento da cadeia de custódia, observa-se que ele foi impropriamente restritivo, já que ao utilizar a terminologia *vestígio* no *caput* e deliminar o seu conceito como "todo objeto ou material bruto, visível ou latente" (§3º, art. 158-A, CPP), acabou não abrangendo as provas digitais ou, até mesmo, a memória humana que, por óbvio, não são brutos (SOUZA; FREIRE, 2020, p. 146).

O legislador também definiu o início da cadeia de custódia, ocorrendo a partir da preservação o local de crime ou através dos procedimentos policiais ou periciais em que seja detectado a existência de vestígio (§1º, art. 158-A, CPP), uma vez que os elementos podem ser encontrados em locais diferentes do local em que ocorreu o crime, a exemplo de vestígios encontrados na roupa, no carro ou na residência do autor do delito (SILVA JÚNIOR, 2022, p. 320). Além disso, foi atribuído a responsabilidade de preservação do local pelo agente público que reconhecer um elemento como de potencial para a produção da prova pericial (§2º, art. 158-A, CPP).

Em sequência, foram fixadas as etapas da cadeia de custódia quanto ao rastreamento do vestígio, disposto no art. 158-B, do CPP, da seguinte forma: a primeira etapa é baseada no reconhecimento, isto é, o agente responsável tem como função identificar e distinguir

determinado elemento como de potencial interesse para a produção da prova pericial (inciso I). Posteriormente, é realizado o isolamento e a preservação desse material e do ambiente imediato, mediato e relacionado aos vestígios e local do crime, para que se evite alterar o estado das coisas, conservando, dessa forma, todo o ambiente ao redor para que não haja interferências de terceiros (inciso II).

Após o isolamento, é realizada a etapa de fixação, descrevendo o vestígio, de forma detalhada, conforme se encontra no ambiente ou no corpo de delito, mencionando a sua posição na área de exames, podendo o agente se utilizar de mecanismos de fotografia, filmagem ou croqui para auxiliá-lo na descrição, porém sendo indispensável a descrição desses instrumentos no laudo pericial produzido pelo perito responsável (inciso III). A coleta ou ato de recolher o vestígio é a próxima etapa da cadeia de custódia e tem como propósito submeter a prova à análise do perito, sempre zelando pelas suas características e natureza (inciso IV).

A quinta etapa para resguardar a cadeia de custódia de determinado vestígio é o acondicionamento, isto é, o perito responsável irá embalar o vestígio, de forma individualizada, de acordo com as suas características físicas, químicas e biológicas, para que seja possível a análise posterior, com a anotação da data, hora e o nome de quem realizou a coleta e o acondicionamento (inciso V). A transferência desse vestígio de um local para outro deve ser realizada através de condições adequadas, como embalagem, veículo e temperatura, de modo a garantir a preservação das características originais, bem como o controle de quem detém a posse desse vestígio (inciso VI).

O ato de recebimento desse vestígio também foi mencionado pelo legislador. Nessa etapa, é necessário documentar com a maior quantidade de informações possíveis, especialmente o número de procedimento, a unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo de vestígio, protocolo, assinatura e identificação de quem recebeu. Todos esses dados são importantes para identificar eventuais erros no procedimento da cadeia de custódia, inclusive o responsável de cada etapa (inciso VII).

Posteriormente, temos o processamento do vestígio que é basicamente o próprio exame pericial. Aqui, o perito, através da metodologia adequada às características biológicas, físicas e químicas, irá manipular o vestígio em busca de obter o resultado desejado e logo depois formalizar todas as informações em um laudo oficial (inciso VIII). Por fim, temos as etapas de armazenamento (inciso IX) e o descarte (X) do vestígio, sendo aquele o procedimento referente à guarda, sempre em condições adequadas à sua manutenção, para realização de contraperícia,

descarte ou até mesmo transferência, e o descarte que é a liberação do vestígio, dependendo de autorização judicial, quando necessário ao caso.

Também foi previsto pelo legislador que a coleta dos vestígios deverá ser realizada, preferencialmente, por perito oficial, sendo o órgão central de perícia oficial de natureza criminal o responsável por detalhar a forma do cumprimento, além de restar proibida a entrada nos locais que foram isolados, bem como a remoção de quaisquer vestígios de locais de crimes, antes da liberação pelo perito responsável. O não cumprimento desses requisitos pode gerar responsabilização por fraude processual, conforme o art. 158-C, do CPP.

O acondicionamento também foi tratado pelo legislador, determinado que cada recipiente deve ser selado com lacre, com numeração individualizada, de forma a garantir a inviolabilidade e idoneidade do vestígio durante o transporte (§1º, art. 158-D, CPP). Também restou definido que o recipiente deverá servir para preservar as características originais do vestígio, evitando a sua contaminação ou vazamento (§2º, art. 158-D, CPP), e que somente será aberto pelo perito responsável ou, motivadamente, por pessoa autorizada (§3º, art. 158-D, CPP). No caso de rompimento do lacre, deverá ser registrado na ficha de acompanhamento, além de ser acondicionado no interior de um novo recipiente (§§4º e 5º, art. 158-D, CPP).

Por fim, os arts. 158-E e 158-F, do CPP, trataram sobre a criação de uma central de custódia destinada à guarda e controle dos vestígios, bem como sobre o armazenamento do material em local diverso, caso a central não possua espaço ou condições necessárias para armazenas um determinado material.

Para fins deste estudo, percebe-se que ao longo do texto inserido nos arts. 158-A a 158-F, do CPP, o legislador acaba restringindo a observância da cadeia de custódia para elementos materiais, encontrados basicamente em crimes já previstos pela redação originária do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, o qual instituiu o Código Penal. Isto é, crimes tradicionalmente cometidos ao longo da história – homicídios, roubos, estupro etc. – são necessariamente englobados pelo legislador ao dispor sobre a cadeia de custódia, mas isso não significa que os crimes que têm surgido atualmente, como crimes cibernéticos, não devem se submeter ou observarem as regras previstas para garantir a idoneidade da produção probatória.

O Superior Tribunal de Justiça, muito antes da vigência do Pacote Anticrime, já se debruçou sobre a aplicabilidade da cadeia de custódia na produção de provas digitais, exemplo disso foi a operação Negócio da China, deflagrada em 2008, em que se investigava o cometimento dos crimes de contrabando, sonegação de impostos e lavagem de dinheiro pelo grupo econômico Casa & Vídeo, objeto do Habeas Corpus nº 160.662, do Rio de Janeiro, de relatoria da Ministra Assusete Magalhães.

A defesa dos impetrantes alegou, no que tange especificamente a esse estudo, a falta de acesso às provas que foram coletadas pelos agentes da Polícia Federal, afirmando o desaparecimento de parte substancial dos áudios telefônicos interceptados, os quais teriam sido apagados por agentes policiais, sem oportunizar o acesso à defesa, ao Ministério Público ou até mesmo ao Poder Judiciário.

A 6ª Turma do Superior Tribunal de Justiça decidiu, portanto, pela anulação das provas produzidas em interceptações telefônicas e e-mails que foram perdidos ou apagados pela Polícia Federal, uma vez que é obrigação do Estado a conservação desse material, de modo a resguardar o devido processo legal e a própria ampla defesa. A ministra esclareceu, ainda, que o fato de a autoridade policial reconhecer que tais documentos não são importantes para a investigação não retira o direito da defesa em ter acesso e conhecer a integralidade da prova colhida.

Nas palavras de Geraldo Prado (2019, p. 11), essa decisão tratou sobre "inédito reconhecimento explícito da relevância de se acionar um dos dispositivos do sistema de controles epistêmicos, na hipótese da *cadeia de custódia de determinadas provas digitais*". Acontece que o rito da cadeia de custódia foi elaborado para as chamadas fontes reais de prova, fazendo com que as provas digitais não estivem resguardadas integralmente por essas regras, de modo que é incontestável a importância da cadeia de custódia para a coleta, manutenção e armazenamento das provas digitais que devem seguir um rito específico, sob pena de inutilização da prova (BADARÓ, 2021, p. 7).

Verifica-se, dessa forma, que o legislador ao descrever a cadeia de custódia, se concentrou em normas genéricas, não incluindo práticas específicas para a coleta, armazenamento e utilização das provas digitais ao longo do processo penal. Nesse sentido, Furlaneto Neto *et al*. (2020)[35] registra a necessidade de aplicação de práticas metodológicas específicas aos vestígios digitais, defendendo a aplicação da Norma ABNT NBR ISO/IEC 27037:2012 (ABNT 2013), em vigor no Brasil a partir do dia 09 de janeiro de 2014, a qual é considerada referência internacional para identificação, coleta, aquisição e preservação de evidências forenses digitais em toda as etapas do processo de investigação.

Essa norma, apesar de não ser de observância obrigatória, é a única norma elaborada pela Organização Internacional de Padronização (ISO) em conjunto com a Comissão Eletrotécnica Internacional (IEC) e reconhecidas pelo Brasil, através da Associação Brasileira de Normas Técnicas (ABNT), que trata sobre a metodologia adequada para realização de perícia

---

35 Documento eletrônico não paginado.

informática forense envolvendo os mais diversos equipamentos e dispositivos digitais (FURLANETO *et al*., 2020).

Badaró (2021, p. 8) explica que o ideal seria que o legislador brasileiro tivesse elaborado uma técnica específica para a coleta e apreensão dessa prova, contudo, diante da ausência de regramento específico, o autor pontua que diante das características das provas digitais, especialmente da sua vulnerabilidade, deve se valer de instrumentos específicos relacionados à chamada *computer forensics* com o objetivo de constituir uma prova utilizável na persecução penal, destacando etapas para a produção da prova digital, de acordo com a normativa da ABNT NBR ISO/IEC 27037:2012.

Em algo similar à cadeia de custódia, mas agora voltada especificamente sobre a prova digital, Badaró (2021, p. 8) destaca que a primeira etapa seria a individualização do suporte informático que contenha o dado digital útil à investigação. Após separar o suporte informático, o perito responsável deverá proceder à obtenção do dado digital, utilizando-se de técnica de interceptação, no caso de fluxo de comunicação, ou de sequestro e cópia ou espelhamento do suporte em que está registrado o arquivo de dados.

A conservação é um dos pontos principais para assegurar a proteção da uma cadeia de custódia da prova digital, isso porque o responsável deverá armazenar os dados digitais obtidos e copiados em um local seguro e adequado. A normativa não especifica qual é o tipo de local ou até mesmo ressalta as condições específicas para a sua manutenção, mas é possível compreender que o perito deverá resguardar a prova digital de forma a evitar a sua deterioração.

Posteriormente, será realizada a análise dos dados obtidos, examinando exclusivamente a cópia do suporte informático, que possua relevância para o objeto da investigação, isto é, deverá ser apontado pelo perito oficial nesse momento a prova digital que possua importância para a resolutividade ou desenvolvimento da investigação criminal. Após essa análise, deverá ser apresentado os resultados da investigação perante o órgão judiciário, mediante a produção de prova pericial e, dependendo da complexidade da matéria e da sua tecnicidade, o perito poderá esclarecer verbalmente eventuais dúvidas em audiência.

Ressalta-se que essa norma serve de embasamento e referencial teórico para o Procedimento Operacional Padrão (POP), adotado pela Secretaria Nacional de Segurança Pública (SENASP), com o objetivo de estabelecer um estudo técnico específico para a realização dessa perícia criminal. Na publicação do POP sobre a informática forense, é possível encontrar disposições e regramentos sobre a forma de exame pericial de mídia de armazenamento computacional, de equipamento computacional portátil, de local de informática e sobre o local de internet.

No que tange especificamente à violação ou não observância de alguma etapa da cadeia de custódia, é possível observar que a doutrina facilmente observa dois caminhos para as provas tradicionais: a sua inadmissibilidade integral ou a valoração da prova que eventualmente tenha sofrido alguma forma de irregularidade leve, concedendo um menor valor à prova produzida, mas não retirando-a completamente do processo penal. No entanto, o legislador, mais uma vez, não forneceu a devida atenção à cadeia de custódia das provas digitais, isso porque, diferentemente das provas habitualmente conhecidas, não há como garantir a originalidade dos dados digitais coletados diante das suas próprias características de fragilidade e volatilidade (BADARÓ, 2021, p. 9).

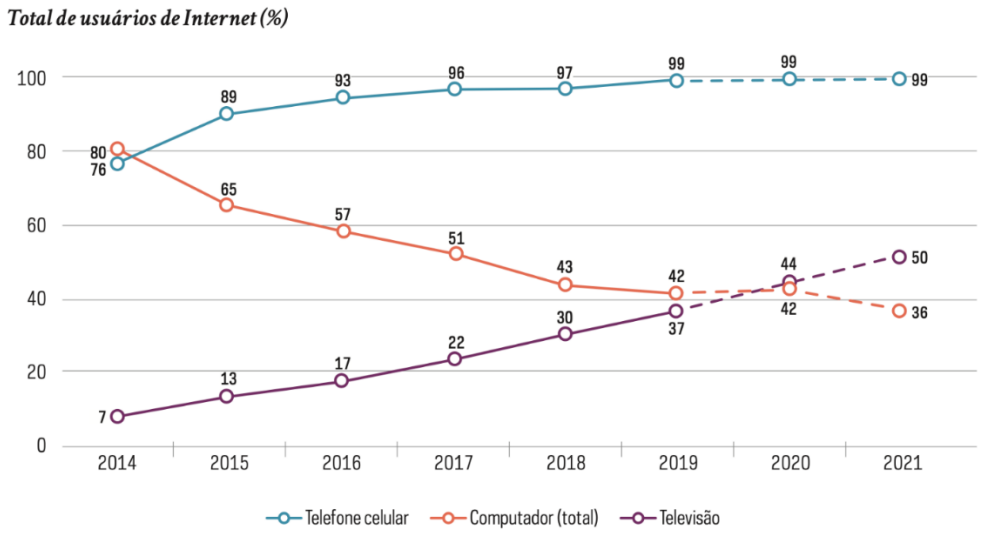
Desse modo, de acordo com os estudos realizados pelo autor Furlaneto *et al*. (2020), a adoção dos padrões estabelecidos pela ABNT NBR ISO/IEC 27037:2012 em conjunto com o POP veiculado pela SENASP, viabiliza a produção da prova digital de forma íntegra e autêntica, o que poderá auxiliar na elucidação de diversos crimes, sem riscos de prejudicar a prova da materialidade da infração ou eivá-la de qualquer vício que possa resultar na sua inadmissibilidade. Para tanto, é imprescindível o aperfeiçoamento da legislação e a capacitação dos servidores do Ministério Público e, especialmente dos agentes das Polícias, a fim de atender a crescente demanda de crimes que estão sendo cometidos através de dispositivos eletrônicos.

4 O USO DE DADOS DE GEOLOCALIZAÇÃO

O desenvolvimento da tecnologia permitiu que 81% (oitenta e um por cento) da população brasileira, no ano de 2021, tivesse acesso à internet, demonstrando, segundo dados da pesquisa sobre o *Uso das tecnologias de informação e comunicação nos domicílios brasileiros* (TIC Domicílios) que o telefone celular foi utilizado por praticamente todos os usuários de Internet (99%) para acessar à rede, em evidente crescimento quando comparado aos anos anteriores. No ano de 2014, o índice de usuários que utilizavam internet através de telefone celular era de 76% (setenta e seis por cento) e esse índice só foi aumentando gradativamente nos anos subsequentes até atingir a porcentagem de 99% (noventa e nove por cento) em 2018, estabilizando até o ano de 2021.

A título de comparação, percebe-se que o índice de usuários que utilizam computador para conexão à internet tem diminuído ao longo dos anos. No ano de 2014, é possível observar que 80% (oitenta por cento) dos usuários utilizam o computador para instrumento de acesso à rede, no entanto, quando comparado ao ano de 2021, verifica-se que o índice caiu para apenas 36% (trinta e seis por cento), enquanto o número de usuários de telefone celular aumentou durante esses sete anos de pesquisa.

Gráfico 5 – Usuários de internet, por dispositivo utilizado (2014-2021)



Fonte: Pesquisa TIC Domicílios (2021).

Apenas para esclarecer o aumento do índice relacionado ao uso da televisão como dispositivo eletrônico para acesso à internet, o relatório gerado pela pesquisa TIC Domicílios (2021) justifica essa constatação inserindo o argumento de que o avanço tecnológico desses

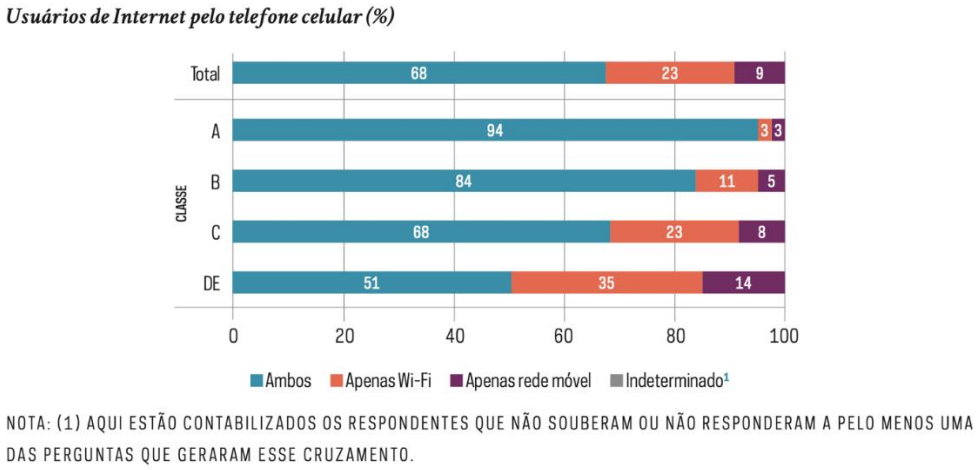
dispositivos para acesso à internet ocasionou um salto de 7% (sete por cento) no ano de 2014 para 50% (cinquenta por cento) no ano de 2021. Esse aumento pode ser justificado pela necessidade dos usuários em acessarem aplicativos de vídeos e séries através das televisões, como por exemplo, *Youtube*, Netflix ou *Globoplay*, aumentando a possibilidade de mídias que podem ser reproduzidas em seu domicílio.

No entanto, regressando à temática desse estudo, observa-se que além do acesso exponencial aos telefones celulares refletirem em uma maior inclusão digital, também é possível verificar consequências expressivas na coleta de evidências durante a investigação criminal. O que antes era transmitido através de mensagens escritas ou comunicações telefônicas, atualmente pode ser retratado através das mensagens instantâneas nos mais diversos aplicativos, o que faz com que o Poder Judiciário tenha que enfrentar mais pedidos de acesso ao conteúdo dos equipamentos eletrônicos apreendidos.

Apesar das mensagens trocadas por indivíduos conseguirem, em alguns casos, corroborar com investigações criminais, o presente tópico dedica-se a abordar especialmente os dados sobre geolocalização que são fornecidas através da conexão com a internet, independentemente dos dados de conteúdo identificados a partir de mensagens enviadas ou recebidas entre potenciais investigados. Para justificar a importância do presente estudo, é necessário verificar o índice de utilização de conexão por internet utilizada por usuários brasileiros.

De acordo com a pesquisa TIC Domicílios (2021), verificou-se que, entre os usuários de internet pelo telefone celular, 68% (sessenta e oito por cento) dos usuários utilizavam as duas formas de conexão, tanto o Wi-Fi quanto a rede móvel, enquanto 23% (vinte e três por cento) se conectava apenas através de Wi-Fi e apenas 9% (nove por cento) utilizada apenas a rede móvel 3G ou 4G para se conectar à internet.

Gráfico 6 – Usuários de internet pelo telefone celular, por tipo de conexão utilizada de forma exclusiva ou simultânea (2021)



Fonte: Pesquisa TIC Domicílios (2021).

Se compararmos a conexão utilizada por classes, é possível verificar, por exemplo, que as classes A e B superaram o patamar de 80% (oitenta por cento) na utilização das duas formas de conexão, enquanto nas classes D e E, apenas metade dos usuários informaram se conectar nesse dispositivo, tanto por meio de Wi-Fi quanto da rede móvel (51%), sendo maior a porcentagem referente àqueles que utilizavam somente da rede Wi-Fi (35%). A pesquisa informa que esse mesmo padrão pode ser encontrado nos cortes por faixa de renda familiar e escolaridade, reforçando o diagnóstico que a parcela economicamente mais vulnerável enfrenta maiores limitações de acesso à internet, mas ainda possuem um número razoável de acesso.

Tem-se, então, o seguinte quadro geral da população brasileira: (i) 81% (oitenta e um por cento) da população brasileira possui acesso à internet; (ii) 99% (noventa e nove por cento) dos usuários de internet acessam através do dispositivo de telefone celular; e (iii) 68% (sessenta e oito por cento) utilizam conexão via Wi-Fi e rede móvel, 23% (vinte e três por cento) utilizam apenas conexão via Wi-Fi e 9% (nove por cento) apenas através de rede móvel (TIC DOMICÍLIOS, 2021).

A partir dessas informações, é possível observar que o acesso a celulares modernos permite que o indivíduo consiga ter acesso à internet em qualquer espaço físico, seja para trocar de mensagens instantâneas, buscar informações e serviços, realizar transações financeiras, pesquisar atividades profissionais, educacionais, culturais e até mesmo utilizar a geolocalização como facilitador para diversas atividades como, por exemplo, obter informações sobre mapas meteorológicos, facilitar a locomoção, utilizar determinado meio de transporte, encontrar a

localização de serviços ou lojas, buscar amigos pelas redes sociais ou até mesmo acompanhar familiares com o fim de resguardar sua segurança.

Machado *et al*. (2021)[36] aborda a importância da utilização de dados coletados por aplicativos nas mais diversas áreas, trazendo, como exemplo, o uso de dados de localização na área da saúde. Os autores ressaltam que a combinação dessas temáticas poderia auxiliar na identificação de áreas que estão mais sujeitas a certos patógenos e, assim, adotar melhores estratégias de prevenção e atendimentos aos pacientes. Além disso, também poderia ser eficaz durante a pandemia de Covid-19, na medida em que utilizando-se de estudos sobre a taxa de infecção de novos casos por região, seria possível auxiliar na contenção do avanço da doença e tratar de forma mais eficiente as áreas afetadas.

Na área criminal, por sua vez, vê-se que a facilitação desse acesso e a portabilidade de dispositivos eletrônicos faz com que a dinâmica da prova obtida nesta seara também se altere, uma vez que as empreitadas criminosas tendem a ser valer dessas facilidades tecnológicas para alcançar seus objetivos. Por outro lado, a utilização dessas facilidades também leva o indivíduo ao compartilhamento, mesmo que não desejado, de informações pessoais ou de terceiros, que permitem identificar a pessoa, o uso do aparelho e a sua localização (SMANIO, 2021, p. 50).

Além de telefones celulares, as tecnologias voltadas ao controle da população como práticas enquadradas como *surveillance*[37], como as câmeras de vigilância e até mesmo os *drones*, localizadas em vias públicas ou em prédios públicos ou privados, também acabam cumprindo um papel relevante na seara investigativa, isso porque mais que auxiliar na captação de imagens, elas também permitem identificar a localização do indivíduo. Não necessariamente com o intuito acusatório, mas também podem servir como instrumento de defesa, comprovando que o indivíduo não esteja no local do crime, mas em outro ambiente.

Outra forma de dispositivos eletrônicos comumente encontrado com a população, são os *smartwatches*, isto é, relógios inteligentes que ganharam popularidade ao permitirem a visualização de mensagens, informações de saúde, rastreamento para atividades físicas (corrida, trilhas, triathlon etc.), tornando um ambiente de facilidade para o usuário, mas também criando nossas oportunidades ao cometimento de crimes no mundo virtual (DE MIRANDA FONSECA; ZAMPOLO, 2022, p. 3). No entanto, no estudo realizado por Miranda Fonseca e Zampolo (2022, p. 11), verificou-se que no âmbito pericial, as investigações desses dispositivos são

---

[36] Documento eletrônico não paginado.

[37] A nomenclatura *surveillance* compreende as "práticas voltadas à vigilância, segurança e manipulação de dados que fazem parte do conjunto de ações dispostas no sentido de gerenciar comportamentos, dados e segurança." (AMARAL; DIAS, 2019, p. 3).

complementares, uma vez que a maior parte desses relógios precisam de um *smartphone* para permitir o acesso a totalidade de suas funções. Apesar disso, o trabalho demonstrou que mesmo uma análise individual foi possível extrair informações importantes, seja como fonte de evidências ou como indicações de provas a serem investigadas durante o procedimento.

Fato é que os dados de localização podem ser encontrados em diversos dispositivos eletrônicos, visto que ao trazer mais conforto ao usuário, também permite o estudo de evidências relacionados aos crimes e geradas em dispositivos digitais. No âmbito legislativo nacional, Lopes Júnior (2021)[38] destaca a inclusão dos arts. 13-A e 13-B no Código de Processo Penal, através da Lei nº 13.344/2016, os quais foram responsáveis por implantar meios específicos de investigação para a apuração dos crimes de tráfico de pessoas (art. 149-A, CP), redução a condição análoga à de escravo (art. 149, CP), sequestro e cárcere privado (art. 148, CP), extorsão com restrição da liberdade da vítima (art. 158, §3º, CP), extorsão mediante sequestro (art. 159, CP) e tráfico internacional de crianças (art. 239 da Lei nº 8.069/90).

Nesses casos, a grande inovação destacada pelo autor foi a possibilidade de obtenção da localização da Estação Rádio Base (ERB), definida como "estação de cobertura, antena ou outro meio similar, acionada quando da realização ou recebimento de chamadas de telefone celular da vítima ou de suspeitos" (LOPES JÚNIOR, 2021)[39]. No entanto, o legislador acabou limitando a utilização desse instrumento para os crimes relacionados ao tráfico de pessoas que esteja em curso, não estendendo aos demais crimes relacionados no artigo anterior (art. 13-A, CPP).

Silva Júnior (2022, p. 142) ao realizar uma análise desses dispositivos, especialmente do art. 13-B, objeto desse estudo, levanta o questionamento sobre a atecnia do legislador ao se referir sobre *crimes relacionados ao tráfico de pessoas* de forma genérica. Se proceder a uma análise do contexto, parece que o legislador teve a intensão de realçar qualquer crime relacionado ao tráfico de pessoas, seja nacional ou internacional, ou até mesmo o caso de tráfico de criança e adolescente, previsto pelo Estatuto da Criança e do Adolescente.

Acontece que a redação precária estimula o leitor a pensar que a regra ali estabelecida é direcionada apenas a esse tipo de delito, de modo que, se investigado qualquer outro tipo penal, não seria possível, sequer com autorização judicial, requisitar os dados de localização, criando, desse modo, uma espécie de inviolabilidade da intimidade ou da vida privada absoluta, o que não deve ser a interpretação adequada. Da leitura do § 4º do art. 13-B, é possível esclarecer que a intenção do legislador foi, na verdade, a de conferir uma amplitude

---

[38] Documento eletrônico não paginado.
[39] Documento eletrônico não paginado.

investigativa maior quando for a hipótese de crime de tráfico de pessoas, não a de restringir o alcance da norma a esse tipo penal (SILVA JÚNIOR, 2022, p. 142).

O dispositivo mencionado dispõe que na ausência de manifestação judicial no prazo de 12 (doze) horas, a autoridade competente poderá requisitar às empresas prestadoras de serviço de telecomunicações e/ou telemática para que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, com imediata comunicação ao juiz.

Acontece que até mesmo dessa leitura, pode-se questionar a sua constitucionalidade, isso porque não é possível que norma infraconstitucional dispense autorização judicial para requisição dessas informações e flexibilize os princípios de inviolabilidade da intimidade e/ou vida privada. No entanto, é necessário relembrar que a intenção do legislador ao prever essa norma é de assegurar meios de investigação para os delitos de tráfico de pessoas, que é um delito permanente e pressupõe situação de flagrante (SILVA JÚNIOR, 2022, p. 142).

Essas informações coletadas através das requisições às empresas prestadoras de serviço de telecomunicações e/ou telemáticas para disponibilizar imediatamente os meios técnicos adequados que permitam compartilhar a localização aproximada da vítima ou do suposto autor do delito, apesar de limitar à aplicabilidade de apenas um delito tipificado na legislação brasileira, demonstram pontos positivos da utilização de dados de localização para uma melhor resolução de uma investigação criminal em curso, como também para a prevenção do cometimento de outros atos ilícitos por parte do suspeito.

4.1 **Delimitação conceitual do instrumento de geolocalização**

Os dados de localização podem ser obtidos através das Estações Rádio-Base (ERB), conforme visto no tópico anterior, ou através do Sistema de Posicionamento Global (GPS), vinculado a algum aparelho eletrônico e gerado através da utilização de determinados aplicativos, o que será ponto principal a ser abordado nesse estudo diante do crescimento do número de usuários que utilizam esses serviços. A utilização desses aplicativos que possibilitam o fornecimento de dados de localização pode ser chamada de serviços de localização, também conhecidos como *location-based services* (LBS) (MACHADO *et al*., 2021)[40].

O crescimento da utilização desses serviços de localização tem contribuído para o compartilhamento de dados dos usuários, especialmente, os dados de localização. Schiller et a.

[40] Documento eletrônico não paginado.

(2004, p. 01) define serviços de localização como aqueles que integram localização geográfica, como coordenadas espaciais, com a noção de serviços gerais, citando, como exemplos, os serviços de emergência, sistemas de navegação de veículos automotores ou mesmo a utilização de mapas.

Dessa forma, percebe-se que os serviços de navegação, através de aplicativos como o *Google maps* ou *waze*, aplicações de tempo para obter informações sobre o clima local, jogos, como o *Pokemon GO*, ou serviços de recomendação, como o *Foursquare* e *Yelp*, facilitam o compartilhamento de dados de localização dos usuários (MACHADO *et al*., 2021)[41]. É um dos aspectos relacionados ao *capitalismo de vigilância*, o qual, em breve síntese, utiliza o compartilhamento desses dados para o aprimoramento de produtos e serviços, conseguindo, inclusive, moldar o comportamento individual, seja para adquirir um determinado produto em uma sexta-feira à noite ou para votar na eleição que ocorrerá na semana seguinte (ZUBOFF, 2021)[42].

Como destacado no tópico anterior, o desenvolvimento de dispositivos móveis, como telefones celulares, equipados com sistema de posicionamento global (GPS), em conjunto com acesso à internet sem fio, tem contribuído para a popularidade de serviços de localização. No âmbito do direito criminal, a popularização do sistema de GPS acabou tornando-a economicamente acessível e de baixo custo, fazendo com que se tornasse uma forma de controle empregada em diversos países, seja como instrumento de tutela cautelar, em qualquer fase de persecução penal ou até mesmo na execução penal, auxiliando no controle do cumprimento de pena (LOPES JÚNIOR, 2020)[43].

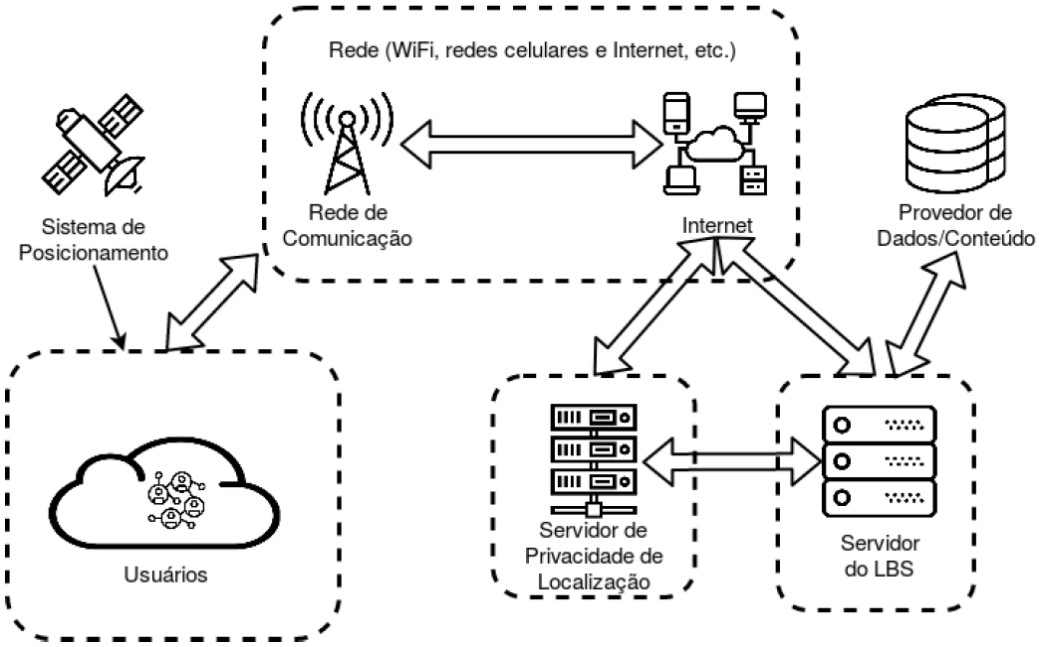
Em regra, o sistema de posicionamento global (GPS), presente na maioria dos dispositivos eletrônicos, consiste em um conjunto de 24 satélites que estão presentes "na órbita da Terra a uma altura de 10.900 milhas, tornando possível às pessoas que utilizem receptores no solo determinar sua posição geográfica entre 10 e 100 metros" (PINHEIRO, 2021)[44]. Dessa forma, o usuário que, através de um dispositivo eletrônico que tenha acesso a uma rede, seja rede móvel ou Wi-Fi, requisitar ou autorizar previamente ao provedor de serviço que forneça determinada operação – como previsão do tempo – compartilhará os dados de localização próprios para facilitar a prestação de serviço, conforme ilustra a figura abaixo (MACHADO *et al*., 2021)[45].

---

41 Documento eletrônico não paginado.
42 Documento eletrônico não paginado.
43 Documento eletrônico não paginado.
44 Documento eletrônico não paginado.
45 Documento eletrônico não paginado.

Importante destacar que a figura mencionada no artigo ilustra um serviço baseado em dados de localização com preservação de privacidade, obtidas através do consentimento do usuário que está utilizando o serviço com o objetivo de garantir uma maior proteção dos seus dados pessoais. No entanto, o que se busca demonstrar com essa ilustração é como é realizado o procedimento de captação dos dados de localização dos usuários de internet através de telefones celulares que disponham do sistema de posicionamento global (GPS).

Figura 1 – Modelo de sistema de serviços baseados em localização



Fonte: Machado e Duarte Neto (2021[46]).

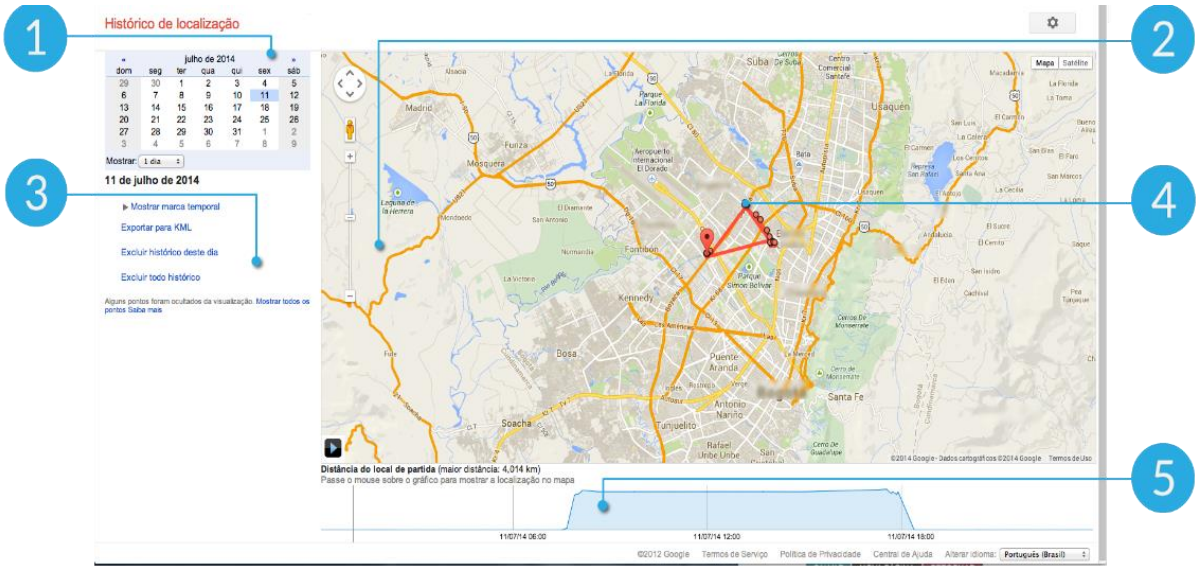
Assim, compreende-se que os dados de localização são concedidos a partir de um servidor do LBS (serviços de localização), o qual é o responsável por receber as requisições dos usuários que possuam um dispositivo eletrônico com o sistema de posicionamento global (GPS), através de uma conexão à internet, seja por Wi-Fi, rede móvel ou até mesmo satélite, e prestar o serviço baseado na localização de acordo com a sua natureza, seja pra encontrar um determinado local, para auxiliar a navegação ou qualquer outra forma que se utilize do posicionamento global (MACHADO *et al*., 2021)[47].

Um dos exemplos desse acesso aos dados de localização pode ser encontrado na ferramenta desenvolvida pela empresa Google. Através do gerenciamento do histórico de

[46] Documento eletrônico não paginado.
[47] Documento eletrônico não paginado.

localização vinculado ao aplicativo *Google maps*, é possível delimitar calendário de localização (ponto 01), isto é, a localização em um dia exato ou durante o período selecionado, o mapa com as informações sobre a localização do aparelho conectado (ponto 02), utilizar ferramentas de administração (ponto 03), verificar pontos de localização (ponto 04) e até mesmo gerar um gráfico sobre o momento em que o usuário esteve em determinado local (ponto 05). No entanto, importante destacar que esse histórico de localização depende de autorização do usuário e compartilhamento dos seus dados com a empresa, assim como funciona grande parte dos aplicativos utilizados através da conexão à rede.

Figura 2 – Histórico de localização do Google



Fonte: GCF Global: histórico de localização do google (2023).

É através das informações coletadas por essas empresas, como o *Google*, que o usuário pode usufruir de diversas finalidades, como informações de trânsito, serviços de alimentação ou anúncios direcionados. Esse tipo de ferramenta tecnológica é conhecido também por *geofencing*, a qual pode ser conceituada como "um perímetro virtualmente definido ao redor de um certo ponto no globo terrestre, uma espécie de "cerca virtual" (MAIA *et al*., 2021, p. 769-770).

Superado o conceito de sistema de posicionamento global e a forma que ela pode ser captada, passemos à análise sobre a classificação doutrinária dos dados de localização. A Convenção de Budapeste, em seu art. 1º, alínea *b*, define *dados de computador* como qualquer representação de fatos, informações ou conceitos que possam se adequar ao processamento de um sistema de computador que inclua um programa capaz de desenvolver uma tarefa. Esses dados podem ser considerados, conforme visto em tópicos anteriores, como fonte de prova

digital a ser utilizado durante a persecução penal e podem conter informações pessoais, seja do usuário, do dispositivo eletrônico, de conteúdo entre dois ou mais interlocutores, e é exatamente por isso que possuem valor para uma investigação criminal ou para formação de opinião do julgador (SMANIO, 2021, p. 56).

A Lei nº 13.709, de 14 de agosto de 2018, a qual dispõe sobre a Lei Geral de Proteção de dados, prevê em seu art. 5º, inciso I, que *dados pessoais* podem ser compreendidos como aquelas informações relacionadas a pessoa natural identificada ou identificável, podendo abordar mais dados que somente aqueles relacionados ao nome, sobrenome, idade ou endereço, desde que relacionado a pessoa identificada ou identificável. Nesse sentido, Smanio (2021, p. 59) assevera que os dados de localização podem ser classificados como dados pessoais, eventualmente vinculados à comunicação e, portanto, abarcados pela proteção de privacidade de dados e, em outros casos, do sigilo das comunicações, caso essa localização esteja vinculada à transmissão de conteúdo comunicativo entre interlocutores.

Isto é, denota-se que existem duas naturezas distintas no que se refere aos dados de localização. Se vinculada ao conteúdo transmitido entre o remetente e o destinatário, os dados abordados nesse estudo terão uma natureza estática e estarão abarcados pelo sigilo de comunicações, previsto no art. 5º, inciso XIII da Constituição, devendo seguir o rito das interceptações de comunicação contida na Lei nº 9.296/96. Por outro lado, se estiver vinculada ao terminal do dispositivo eletrônico utilizado, ou for informação de localização armazenada, o dado será dinâmico e estará protegido pela privacidade, inserido no art. 5º, inciso X, da Constituição Federal e será regulamentado pelo art. 13-B do Código de Processo Penal (SMANIO, 2021, p. 60).

Na análise da utilização de dados de localização na seara criminal, o principal questionamento é a possibilidade do indivíduo em simplesmente desligar os dados de localização contidos em seu telefone celular ou até mesmo a dificuldade em conseguir acesso a essas informações através das pessoas jurídicas responsáveis por este armazenamento. A problemática que envolve o primeiro ponto pode ser debatida diante da necessidade dos usuários em acessar determinados serviços pelo telefone celular e, involuntariamente, compartilhar dados de localização. Logo, apesar de não possuir, na maioria das vezes, um histórico detalhado como o elaborado pelo aplicativo *Google maps*, é possível identificar o local específico que o indivíduo requisitou determinado serviço ou utilizou determinado aplicativo para se comunicar, possibilitando o uso dessas informações para corroborar as investigações criminais.

O segundo ponto levantado talvez seja a maior problemática enfrentada pelos órgãos investigativos com maior capacidade estrutural, isso porque, na maioria das vezes, as requisições elaboradas às empresas detentoras das informações geradas através da utilização de dispositivos eletrônicos não são atendidas ou, no caso de serem, demoram meses, o que torna a investigação criminal obsoleta.

No Brasil, o Instituto de Referência em Internet e Sociedade (IRIS) instituiu uma plataforma de monitoramento de casos concretos que envolveram bloqueios ou requisições para bloqueios de aplicações de Internet no país. A plataforma publicou o primeiro, de quatro casos já registrados sobre o mesmo aplicativo, de descumprimento de ordem judicial para entrega de dados de usuários, o qual envolveu o *Whatsapp*. A primeira decisão de bloqueio, publicada no ano de 2015, teve origem na Central de Inquéritos de Piauí, mas não chegou a ser implementada já que diversos mandados de segurança requerendo a sua suspensão foram impetrados por provedores de internet que estariam a cargo de executar o bloqueio (INTERNETLAB).

Os outros três casos aconteceram entre os anos de 2015 e 2016 e nesses foram determinados os bloqueios pelo mesmo motivo – descumprimento de ordens judiciais de acesso a dados de usuário. No entanto, apesar de lograrem êxito na efetivação do bloqueio do aplicativo, as ordens duraram no máximo 24 (vinte e quatro) horas, em virtude de pedido de reconsideração elaborado pelo *Whatsapp*, afirmando, em resumo, que (i) é tecnicamente impossível desabilitar a chave de criptografia de apenas alguns usuários sem comprometer a segurança de todos; (ii) apenas possuem obrigação de armazenar informações referente à data e hora do aplicativo a partir do IP pelo prazo de seis meses; (iii) a suspensão é desproporcional por ferir direitos à comunicação e liberdade de expressão de milhares de usuários brasileiros; (iv) a suspensão da decisão de bloqueio é uma limitação da liberdade de escolha dos consumidores e uma interferência da livre concorrência e por fim, (v) alegou que existem outras medidas de investigação a serem utilizadas pelos órgãos investigativas que não tinham sido esgotadas.

O caso mais recente publicado pela plataforma foi relacionado ao aplicativo *Telegram*. Nessa situação, o Ministro do Supremo Tribunal Federal, Alexandre de Moraes, determinou o bloqueio do aplicativo por descumprimento de diversas ordens judiciais, inclusive a entrega de dados de usuários, por tempo indefinido. Acontece que, nesse caso concreto, a decisão de suspensão do bloqueio aconteceu três dias depois, em virtude do cumprimento integral por parte da empresa, consignando apenas que não armazena dados relacionados aos perfis.

Nesse sentido, Razera (2021, p. 159-161), ao realizar um estudo sobre a dificuldade do acesso a dados criptografados no contexto de investigações criminais, ressalta a importância

de modernização do Estado com o objetivo de preservar os poderes de investigação. O autor destaca que os órgãos de persecução penal devem despertar o olhar para a necessidade de adaptar o aparato investigativo de modo a funcionar na presença de elementos protegidos por criptografia, utilizando dados acessíveis nas plataformas de comunicação, como os metadados, empregando técnicas de infiltração virtual e também buscando soluções para contornar essa linguagem criptográfica mediante serviços de computação em nuvem ou através da exploração de vulnerabilidade de sistemas e aparelhos.

No entanto, para proceder à implementação de uma qualificação técnica voltada às novas tecnologias, é necessário delimitar a produção e o uso desses dados digitais, especialmente os dados de localização, nos termos das diretrizes constitucionais, com o objetivo de resguardar a utilização lícita dessas provas durante a persecução penal.

4.2 **Garantias constitucionais como limite à produção e uso de dados de localização**

A existência de diferentes técnicas de obtenção dos dados de localização do indivíduo – triangulação das estações de rádio base ou acesso à geolocalização através do sistema de posicionamento global – permite a discussão sobre a existência de regulamentação legal para a produção dessas provas no âmbito criminal. Apesar das técnicas de triangulação das estações rádio base serem, de fato, as mais conhecidas e utilizadas por órgãos investigativos, as técnicas mais modernas, como a obtenção de geolocalização em tempo real estão ganhando espaço no âmbito da segurança pública e das investigações criminais.

Acontece que a utilização do sistema GPS e a necessidade constante de comunicação de dados, especialmente a localização em tempo real ou o acesso às informações armazenadas em alguma plataforma, potencializam a violação da privacidade, intimidade e do sigilo das comunicações, além de permitir à autoridade policial saber exatamente o local onde a pessoa está ou esteve naquele lapso temporal (SMANIO, 2021, P. 63). Essa problemática gira em torno, mais uma vez, do descompasso entre o avanço tecnológico, inclusive em técnicas de investigação, e da legislação criminal, uma vez que esta não consegue se desenvolver na mesma velocidade para estipular critérios e definir limites que protejam os direitos fundamentais dos indivíduos eventualmente investigados.

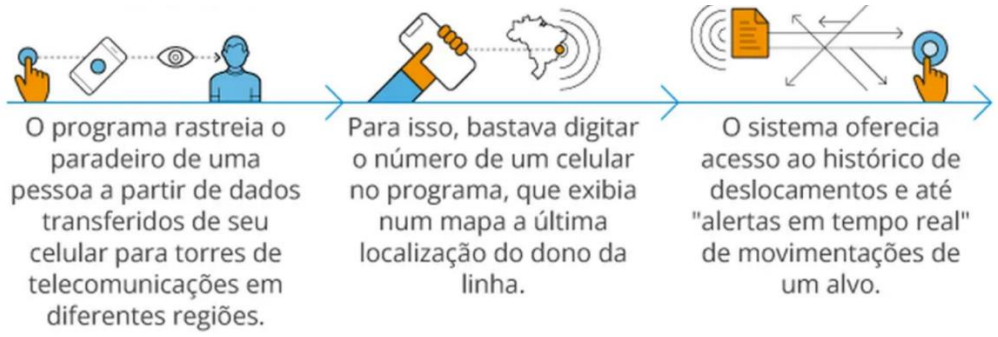
Para Prado (2020, p. 64), a geolocalização – obtenção de dados de localização em tempo real ou armazenada em plataformas digitais – viabiliza uma forma de vigilância extrema do indivíduo em uma sociedade que massivamente faz uso da rede mundial de dispositivos eletrônicos, fazendo com que a privacidade e a intimidade sejam afetadas por uma investigação

criminal, sem sequer possuir um dispositivo legal que regulamente a forma de obter esses dados. Nesse sentido, o autor destaca a importância do papel desempenhado pelo Poder Judiciário que tem sido convocado, com frequência, para decidir sobre quando, de que forma, para que fins e por quanto tempo o Estado, através dos seus agentes, poderá exercer válida e de modo legítimo esses novos meios de obtenção de prova.

Assim, a tecnologia que pode ter ganhado forças no aspecto comercial, mostrou-se valiosa em situações em que as investigações criminais não conseguiram avançar por não conseguir identificar algum suspeito, como é o caso de crimes de homicídio ou estupros que, por vezes, são cometidos sem que se possa encontrar elementos de prova que levem a algum suspeito, como testemunhas, filmagens ou impressões de DNA, por exemplo, sendo necessária a adoção de técnicas especiais de investigação para possibilitar o desenvolvimento das investigações de forma eficiente (MAIA *et al*., 2020, p. 770).

Nesse ponto, o acompanhamento em tempo real dos dados de localização ainda não foi fruto de muitas discussões no âmbito do Poder Judiciário, sendo possível destacar apenas, como exemplo, o recente caso da Agência Brasileira de Inteligência (Abin) que utilizou um sistema secreto para monitorar a localização de cidadãos em território nacional durante os três primeiros anos do governo do ex-Presidente Jair Bolsonaro. De acordo com a matéria publicada, em 14 de março de 2023, na plataforma jornalística *O globo*, a ferramenta, chamada *FirstMile*, desenvolvida pela empresa israelense Cognyte e utilizada pela Abin permitia, através da mera digitação de um contato telefônico no programa, controlar os passos de até 10 mil usuários de telefones celular a cada 12 (doze) meses, conforme demonstra a figura ilustrativa abaixo:

Figura 3 – Funcionamento da ferramenta FirstMile



Fonte: O Globo. Abin de Bolsonaro usou programa secreto para monitorar localização de pessoas por meio do celular (2023).

A utilização da ferramenta não possuía qualquer regulamentação legal ou protocolo oficial e poderia ser utilizada sem necessidade de registro, o que permitia que qualquer usuário com conexão à internet que utilizasse um celular pudesse ser monitorado pelo programa sem uma justificativa oficial. A Abin, por sua vez, confirmou a utilização da ferramenta e informou que o uso teve início em 26 de dezembro de 2018 e foi encerrado em 8 de maio de 2021. Atualmente o caso está sob investigação da Polícia Federal e do Ministério Público Federal, ainda sem conclusão sobre a possibilidade de criminalização de determinadas condutas.

A busca por localização reversa, em contrapartida, já foi objeto de discussão nos Tribunais Superiores. Nesse tipo de busca, o magistrado requisita os dados de localização ao servidor dos IPs de todos os usuários que possuíam qualquer tipo de conexão – rede móvel ou Wi-Fi – e se encontram em um local específico e em determino lapso temporal (SMANIO, 2021, p. 64). É, basicamente, o acesso à dados de localização que se encontram armazenados nas plataformas dos provedores de serviço.

Diante da grande porcentagem de usuários que utilizam telefones celulares para acesso à internet – 99% (noventa e nove por cento), de acordo com a pesquisa realizada pela TIC Domicílios em 2021 – as autoridades começaram a solicitar de empresas como o Google informações de usuários de seus serviços que se encontravam no perímetro que circunda pontos importantes para a investigação, como o local em que tenha sido encontrado o corpo de uma vítima ou o local onde foi encontrado pertences de uma vítima de roubo, por exemplo (MAIA *et al*., 2020, p. 770).

A principal polêmica desse tipo de requisição é o fato de que estão sendo solicitadas informações de todos os usuários que estiveram no local usando um dispositivo eletrônico associado a serviços do Google, independentemente de qualquer vinculação ao fato típico. Nesse ponto, o poder estatal teria acesso às informações atinentes à privacidade dos indivíduos que, muito provavelmente, não cederem os seus dados à Google para serem vigiados e muito menos concordaram em produzir elementos em seu desfavor em um processo criminal (MAIA *et al*., 2020, p. 770).

Além disso, há ainda a problemática referente ao desvirtuamento da medida, uma vez que os agentes poderiam utilizar essas informações com a finalidade de vigilância ou até mesmo perseguição de determinados usuários, se aproximando a uma forma de estado totalitário e policialesco, violando expressamente os aspectos constitucionais promulgados no ano de 1988.

Consideremos, à título de exemplo, o caso de agentes policias integrantes de grupos de milícias que possuam acesso aos dados e informações sobre pessoas que estão sendo monitoradas eletronicamente e, sob o pretexto de garantir segurança pública, passam a

intimidade, extorquir e até mesmo executar as pessoas que possuem a sua localização compartilhada com órgãos públicos. Facilmente, seria possível observar o fortalecimento desses grupos a partir do acesso indiscriminado aos dados, sem qualquer forma de controle ou restrição.

Se considerarmos, ainda, o ambiente de violência doméstica em que o autor do fato faz parte do quadro de agentes policiais e que, prontamente, possui acesso aos dados de localização da vítima, seja através de um acesso direto ou de comunicação com outros agentes, é naturalmente perceptível que a vítima sai de um patamar de proteção de mulheres vítimas de violência doméstica a um local de fragilidade, tornando-se um alvo fácil para o cometimento de novos crimes.

Em qualquer dos casos, é potencial o dano que pode ser causado aos direitos fundamentais individuais por acesso indiscriminado de agentes policiais, isto é, a falta de delimitação de quem deve acessar esses dados e informações de pessoas monitoradas eletronicamente. Em razão disso, torna-se cada vez mais necessário discutir sobre a regulamentação da tecnologia e o impacto aos direitos preservados em um regime democrático.

Preocupado com essa temática, o Conselho Nacional de Política Criminal e Penitenciária do Ministério da Justiça e Segurança Pública (CNPCP/MJSP) publicou a Resolução nº 31, de 1º de dezembro de 2022, a qual regulamenta a implementação, acompanhamento, fiscalização e encerramento das medidas de monitoração eletrônica, decorrentes de ordens judiciais, estabelecendo, inclusive, providência em caso de descumprimento das condições impostas, estabelecendo diretrizes no âmbito do Departamento Penitenciário Nacional (DEPEN) e das administrações penitenciárias.

Ao longo do texto, foi estabelecido procedimentos para padronização das atividades de monitoração eletrônica, decorrentes de ordens judiciais, realizadas pelas Centrais de Monitoração e geridas pelo DEPEN e pelas administrações penitenciárias das unidades federadas (art. 1º). Destaca-se a atribuição exclusiva de servidores públicos do sistema penitenciário para o exercício da atividade de monitoração eletrônica, especialmente as atividades de acompanhamento e fiscalização (§2º, art. 2º), deixando a cargo somente desses servidores o acesso às informações sensíveis oriundas do monitoramento.

Em que pese a resolução tratar ainda sobre a preservação do sigilo dos dados e das informações da pessoa monitorada, faz-se necessário um maior controle e rigidez no tratamento e acesso a esses dados. A possibilidade de criação de um banco de dados para armazenar dados básicos sobre os servidores, como nome, matrícula, dia, horário e a pessoa monitorada que

obteve seus dados acessados, podem ser imprescindíveis para resguardar a segurança e o sigilo tanto do monitorado como de sua família que acaba sofrendo por via reflexa.

Com o objetivo de sanar eventuais lacunas, cita-se aqui a Resolução nº 412, de 23 de agosto de 2021, do Conselho Nacional de Justiça (CNJ), a qual estabeleceu diretrizes e procedimentos para a aplicação e o acompanhamento da medida de monitoramento eletrônico de pessoas. Foi determinado, especialmente, em seu art. 13 que a coleta de dados através do acompanhamento das medidas de monitoramento eletrônico possuem finalidade específica, qual seja, o cumprimento das condições estabelecidas em âmbito judicial e podem ser utilizados como meio de prova para apuração penal, mas estando abrangidos, de qualquer forma, pelo direito à inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, previsto no inciso X do art. 5º, da Constituição Federal, além da legislação de proteção de dados pessoais.

A resolução destaca, ainda, que os sistemas de registro de informações do monitoramento eletrônico serão estruturados com base na preservação do sigilo dos dados e das informações da pessoa monitorada, da pessoa em situação de violência doméstica e familiar e de terceiros (§1º, art. 13), em consonância com o que dispõe a resolução do CNPCP. Em relação ao compartilhamento desses dados e informações, inclusive com instituições de segurança pública, o CNJ esclarece a imprescindibilidade de autorização judicial, mediante a representação da autoridade policial ou requerimento do Ministério Público.

Desse modo, é nítida a preocupação legislativa sobre a regulamentação de acesso aos dados digitais, fazendo com que tanto o CNJ como o CNPCP estabeleçam diretrizes suficientes para regulamentar esse ambiente contra eventuais arbitrariedades e ilegalidades que possam surgir da manipulação dessas informações. Denota-se que as duas resoluções citadas se complementam com o objetivo de resguardar os dados e informações sobre as pessoas acompanhadas através do monitoramento eletrônico, estabelecendo, inclusive, a necessidade de autorização judicial para o compartilhamento desses dados a outros órgãos públicos de segurança pública.

Um caso conhecido em âmbito nacional foi o homicídio da vereadora Marielle Franco e Anderson Gomes, motorista à época, bem como a tentativa de homicídio de Fernanda Gonçalves Chaves, assessora da vereadora à época, ambos ocorridos no dia 14 de março de 2018, na cidade do Rio de Janeiro. Diante das investigações, a 4ª Vara Criminal da Comarca do Rio de Janeiro determinou a empresa Google o fornecimento de informações de usuários de seus serviços que transitaram sobre certos locais da cidade com o objetivo de proporcionar a identificação dos usuários ou de terminais utilizados.

Apesar do processo se encontrar sob sigilo, foi noticiado pelo portal do Superior Tribunal de Justiça (STJ) que a empresa Google interpôs recurso visando a reconsideração dessa decisão do Juízo de primeiro grau, alegando para tanto que o ordenamento jurídico brasileiro não admite quebras de sigilo e interceptações genéricas, sem a individualização das pessoas afetadas, e que tal medida contrariaria a proteção constitucional conferida à privacidade e aos dados pessoais.

No entanto, a Terceira Turma do STJ, sob a relatoria do Ministro Rogério Schietti Cruz, nos autos do RMS 61302/RJ, negou provimento ao recurso e manteve a decisão que determinou o compartilhamento dessas informações, sob o argumento de que é possível flexibilizar o direito ao sigilo quando presentes circunstâncias que demonstrem a existência de interesse público relevante e de decisão judicial suficientemente fundamentada que justique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal. O Ministro destacou, ainda, que a determinação do juiz de primeira instância foi para a quebra de sigilo de dados estáticos, isto é, dados armazenados pelos provedores referente ao perímetro geográfico percorrido pelos usuários, e não a interceptação dos dados de conteúdo da comunicação estabelecidas entre interlocutores, de modo que estaria embasado nos arts. 22 e 23 do Marco Civil da Internet.

Os artigos supramencionados se referem à requisição judicial de registros e, especialmente o art. 22, dispõe que o requerimento não precisa individualizar as pessoas investigadas, mas somente apresentar fundados indícios da ocorrência do ilícito (inciso I), justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória (inciso II) e o período ao qual se referem os registros (inciso III), cabendo ao magistrado garantir o sigilo das informações recebidas e da preservação da intimidade, vida privada, honra e imagem do usuário (art. 23).

O julgamento, todavia, registrou um voto divergente proferido pelo Ministro Sebastião Reis Júnior, em que se questionou a evidente quebra de sigilo e da privacidade de usuários, uma vez que a intenção do Ministério Público é, através de uma ordem genérica e sem delimitação temporal razoável, identificar pessoas a partir do cruzamento de dados. Smanio (2021, p. 71) pontua que o voto do ministro acolhe melhor as questões constitucionais e legais apontadas, na medida em que a busca reversa pela localização é uma medida restritiva de direitos fundamentais, mesmo que submetida à reserva de jurisdição prévia, e que merece ser melhor debatida e regulamentada diante da atipicidade legal.

Por outro lado, Maia *et al*. (2020, p. 778-780) esclarece que o principal propósito da ordem de quebra de sigilo com base em coordenadas geográficas (também conhecidas como

geofence warrant) é justamente encontrar suspeitos em processos nos quais não se tem nenhuma pista sobre a autoria. Para tanto, o autor elucida o método utilizado na análise dos dados obtidos a partir desse modo de investigação, aduzindo que ao receber esse tipo de requisição, o provedor pode identificar os dispositivos encontrados de acordo com os parâmetros geográficos definidos somente com números de identificação anônimos. Posteriormente, é possível que as autoridades investigativas realizem uma filtragem e apontem um menor número de dispositivos relevantes à investigação, demonstrando ao Poder Judiciário os motivos pelos quais aqueles dispositivos são importantes, pedindo, ao final, a quebra do sigilo dos dados pessoais somente daqueles IDs específicos.

Todavia, o autor destaca que apesar das modernas técnicas de investigação possibilitarem uma rápida solução investigativa e processual, é importante deixar claro que o Estado continua sendo o detentor do ônus da prova, ou seja, as autoridades competentes continuam com a responsabilidade de provar que os indivíduos que estava próximo ao local do crime e durante o momento dos fatos possui, indubitavelmente, alguma vinculação o fato típico cometido.

Outro exemplo célebre que pode ilustrar esse tipo de requisição de dados foi a lamentável invasão aos prédios do Congresso Nacional, Palácio de Planalto e ao Supremo Tribunal Federal no dia 8 de janeiro de 2023. Em decorrência deste ato, a Advocacia-Geral da União requereu, no âmbito do Inquérito nº 4.879 do Distrito Federal, que as empresas de telecomunicações, em particular as provedores de serviço móvel pessoal, armazenem pelo prazo de 90 (noventa) dias os registros de conexão suficientes para a definição ou identificação de geolocalização dos usuários que estavam nas imediações da Praça dos Três Poderes e do Quartel-General do Distrito Federal para apuração de responsabilidade na data dos atos cometidos, a qual foi deferida pelo Ministro do Supremo Tribunal Federal, Alexandre de Moraes.

Os casos citados nesta pesquisa demonstram que apesar das decisões dos Tribunais Superiores estarem deferindo requerimento para obtenção dos dados de localização de usuários indiscriminados com base em dispositivos do Marco Civil da Internet na tentativa de regulamentar a medida, a verdade é que a ausência de procedimento específico previsto em lei pode tornar a aplicabilidade dessas medidas restritivas a direitos fundamentais como à privacidade e à intimidade, passíveis de nulidade, uma vez que são baseadas em regramentos analógicos, sem dar importância à natureza e às especificidades da medida no âmbito criminal (SMANIO, 2021, p. 72).

Desse modo, é preciso analisar os direitos à privacidade e à intimidade sob a complexidade dos temas atuais, isso porque por mais que possam ser parâmetros para a limitação da obtenção e produção de provas digitais, especialmente relacionadas à geolocalização, a verdade é que devem ser observadas também sob o viés coletivo, denominado autodeterminação informativa, abordada no tópico 2.2 da presente dissertação.

4.3 **A convenção de Budapeste como parâmetro para legislações domésticas: regulamentação da utilização de dados de localização**

A Convenção de Budapeste, a qual dispõe sobre o Crime Cibernético e dá outras providências foi promulgada na República Federativa do Brasil em 12 de abril de 2023, através do Decreto nº 11.491. Além do Brasil, a Convenção já foi assinada por mais de 60 (sessenta) países e é utilizada por mais de 160 (cento e sessenta) países como orientação para as suas legislações domésticas, sendo sua maioria membros da União Europeia, além de outros membros importantes como Estados Unidos, Canadá, Japão e na América do Sul, Colômbia, Argentina, Paraguai e Chile (COLTRO *et al*., 2021, p.110) O documento é responsável pela previsão de criminalização de diversas condutas no âmbito digital, além de prevê normas sobre investigação e produção de provas eletrônicas e os meios de cooperação internacional (FONSECA, 2022, p. 55).

Fonseca (2022, p. 58-59) elabora um breve histórico dos antecedentes da Convenção de Budapeste, explicando que no ano de 1989, através da 428ª reunião do Comitê dos Ministros dos Estados-Membros do Conselho da Europa, foi publicada a Recomendação nº R (89) 9[48], a qual aconselhava a esses Estados membros realizarem uma revisão em suas legislações domésticas para abordar os Crimes Informáticos, além de orientar sobre a importância de trocar experiências sobre práticas judiciais para a cooperação jurídica internacional sobre esses crimes. Para fins desse estudo, destaca-se a 543ª reunião do mesmo conselho, em que foi publicada a Recomendação nº R (95) 13[49] destacando a necessidade dos países membros em fortalecerem a cooperação internacional, através de normas processuais penais compatíveis com o avanço tecnológico no ambiente digital, inclusive abordando sobre a coleta dessas provas eletrônicas.

Posteriormente, o autor esclarece que o Comitê Europeu para os Problemas Criminais (CDPC), através da criação de um comitê específico para essa matéria no ano de 1996, e da

[48] Disponível em: https://rm.coe.int/09000016804f1094. Acesso em 23 abr. 2023.
[49] Disponível em: https://rm.coe.int/16804f6e76. Acesso em 23 abr. 2023.

criação do Comitê de Especialistas sobre a Criminalidade no Ciberespaço (PC-CY) no ano de 1997, foi compilado esforços para a produção de um projeto de convenção internacional sobre o cibercrime, finalizando com a aprovação de um memorando explicativo preliminar e a revisão de um projeto de Convenção.

Nesse sentido, conforme disposto no Preâmbulo da Convenção, ciente das profundas mudanças desencadeadas pela digitalização e globalização do mundo digital, buscou com a criação dessa normativa incentivar a criação de uma "política criminal comum destinada à proteção da sociedade contra o crime cibernético, nomeadamente pela adoção de legislação apropriada e pela promoção da cooperação internacional, entre outras medidas". Ressaltando, especificamente, a observância e respeito aos direitos humanos fundamentais previstos na Convenção Europeia para a Proteção dos Direitos Humanos e Liberdades Fundamentais, de 1950, o Pacto das Nações Unidas sobre Direitos Civis e Políticos, de 1966, bem como outros tratados internacionais sobre direitos humanos que assegurem o direito à liberdade de consciência e à liberdade de expressão, bem como os direitos à intimidade e à privacidade.

No que se refere à sua disposição, a Convenção de Budapeste possui quatro capítulos, sendo eles: (i) utilização de terminologias, (ii) medidas a serem implementadas a nível nacional, (iii) cooperação internacional e (iv) disposições finais. No presente estudo será dado ênfase ao segundo capítulo, especialmente no que se refere às normas de direito processual penal.

Apenas a título de conhecimento, o primeiro aborda as terminologias utilizadas nas legislações, definindo, sem seu art. 1º, os conceitos de *sistema de computador*, *dado de computador*, *provedor de serviços* e *dados de tráfego*. O capítulo seguinte, responsável por abordar as medidas a serem adotadas nas jurisdições nacionais, é dividido entre as matérias de direito penal, processual penal e jurisdição. Na seção de direito penal, o legislador dividiu a tipificação de condutas nas seguintes classes: crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador, crimes informáticos, crimes relacionados ao conteúdo da informação, violação de direitos autorais e de direitos correlatos, além de abordar outras formas de responsabilidade e sanções.

Na seção referente ao direito processual penal, foram previstas várias adaptações na forma procedimental. A seção é dividida em cinco títulos, sendo eles: (i) disposições gerais, (ii) preservação expedita de dados armazenados em computador, (iii) ordem de exibição, (iv) busca e apreensão de dados de computador e (v) obtenção de dados de computador em tempo real. Os quatro últimos já foram abordados no tópico 3.2, em que se analisou os meios de obtenção de prova tanto do Código de Processo Penal brasileiro como também da Convenção de Budapeste.

Neste tópico, serão abordadas as medidas contidas no título 1, as quais se referem às disposições gerais para o processo penal doméstico.

O art. 14 da Convenção se refere ao âmbito de aplicação dos dispositivos processual, pontuando a responsabilidade do Estado membro na adoção de medidas legislativas compatíveis para a promoção de investigações e processos criminais (parágrafo 1º). O parágrafo seguinte aborda a aplicabilidade da interceptação de dados de conteúdo (art. 21) aos crimes tipificados nos arts. 2 a 11 da Convenção, a outros crimes cometidos por meio de um sistema de computador, bem como pode ser utilizada para a coleta de provas eletrônicas da prática de um crime. O último parágrafo deste artigo menciona o direito de reserva do Estado membro na adoção das medidas de obtenção de dados de tráfego em tempo real (art. 20) e da interceptação de dados de conteúdo (art. 21), esclarecendo no inciso II que qualquer outro Estado pode opor óbice a essa reserva, com o objetivo de possibilitar a mais ampla aplicação das medidas mencionadas anteriormente.

O art. 15, por sua vez, sistematiza a sujeição da implementação desses procedimentos na legislação doméstica às condições e garantias de proteção aos direitos humanos e às liberdades públicas, incluindo os direitos que o Estado membro tenha assumido na Convenção do Conselho da Europa para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, de 1950, na Convenção Internacional da ONU sobre Direitos Civis e Políticos, de 1966, e em outros instrumentos internacionais de direitos humanos, e que tais poderes e procedimentos incorporarão o princípio da proporcionalidade.

O parágrafo segundo prevê que entre essas condições e garantias estarão presentes o controle judicial ou supervisão independente, fundamentação da aplicação e a limitação do âmbito de aplicação e da duração dos poderes ou procedimentos utilizados. Por fim, é mencionado a conformidade ao interesse público e a boa administração da justiça quando analisado o impacto desses poderes e procedimentos previstos sobre os direitos, obrigações e interesses legítimos de terceiros.

Dessa forma, a adesão do Brasil à Convenção de Budapeste demonstra o interesse em adaptar a sua legislação interna de acordo com um novo contexto de evolução tecnológica, especialmente no que se refere à criminalização de novas condutas e ao uso de dados digitais como prova para persecução penal. A única problemática na adequação da legislação a essa Convenção e que demandaria um estudo específico sobre o tema, relaciona-se com a política de encarceramento em massa, isso porque a Convenção determina que as condutas tipificadas como crimes sejam passíveis de sanções eficazes, incluindo a possibilidade de aplicação de penas privativas de liberdade, o que poderia agravar a realidade fática brasileira (COLTRO *et*

al., 2021, p. 117). O autor pontua a importância de se observar a convenção, mas também menciona a necessidade de tratar a pena privativa de liberdade como *ultima ratio* do direito criminal, devendo ser dispendida uma atenção especial à necessidade de medidas penais alternativas ao encarceramento.

Além desse ato, o país também demonstrou preocupação com a temática ao elaborar o Anteprojeto de Lei de Proteção de Dados para a segurança pública e investigação criminal (LGPD Penal). O texto foi elaborado pela Comissão de Juristas instituída através de ato do Presidente da Câmara dos Deputados, em 26 de novembro de 2019, mas até o presente momento ainda continua em trâmite na Câmara dos Deputados.

Destaca-se que a LGPD Penal não foi tratada na Lei Geral de Proteção de Dados (Lei nº 13.709/2018) justamente pelo fato de que foi expressamente prevista a necessidade de lei específica para esse tema. O art. 4º, inciso III, dispôs que a lei não se aplica ao tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, de modo que se tornou necessária a elaboração de uma legislação específica para tratar sobre o tema, sob o fundamento de que os órgãos responsáveis por atividades de segurança pública e de investigação e repressão criminais possuam segurança jurídica para exercer suas funções de forma eficiente e compatível com os direitos fundamentais dos titulares dos dados digitais envolvidos.

A exposição de motivos do Anteprojeto da LGPD Penal destaca que o projeto é estruturado em 12 (doze) capítulos, com 68 (sessenta e oito) artigos, inspirando-se na própria Lei Geral de Proteção de Dados e na Diretiva 680/2016, da União Europeia, que regulou o tratamento de dados para fins de segurança pública e persecução penal, de forma separada ao tratamento de dados como um todo. Nesse sentido, visa introdução normas gerais e complementares às normativas já existente em âmbito nacional, como a regulamentação de quebras de sigilo no contexto do processo penal, como a Lei das Interceptações Telefônicas e Telemáticas, a Lei Complementar nº 105, a qual dispõe sobre o sigilo das operações de instituições financeiras, o Marco Civil da Internet, entre outras), de modo a modernizar de acordo com a nova realidade tecnológica e aprimora-las com vistas a garantir maior segurança jurídica a todos os envolvidos.

Os temas tratados nos capítulos do Anteprojeto da LGPD Penal foram os seguintes: (i) disposições preliminares; (ii) tratamento de dados pessoais; (iii) os direitos dos titulares de dados pessoais; (iv) os agentes de tratamento de dados pessoais; (v) segurança e sigilo dos dados; (vi) acesso à informação e transparência; (vii) tecnologias de monitoramento e tratamento de dados de elevado risco; (viii) compartilhamento de dados; (ix) transferência

internacional de dados e cooperação internacional; (x) unidade especial de proteção de dados em matéria penal; (xi) sanções, e (xii) disposições finais de transitórias.

No que tange ao objeto desse estudo, o capítulo VII ao abordar as tecnologias de monitoramento e tratamento de dados de elevado risco, previu inicialmente a necessidade de previsão legal específica, a qual estabeleça garantias aos direitos dos titulares e seja precedida de relatório de impacto de vigilância (art. 42). A obtenção de dados de localização pode ser enquadrada como consequência de um capitalismo de vigilância, no qual a partir do desenvolvimento de uma tecnologia de monitoramento (GPS, por exemplo) é possível acompanhar os locais que determinado indivíduo frequentou, de modo que será abordado as diretrizes estipuladas nesta temática pelo anteprojeto.

Nesse ponto, a LGPD Penal dispôs que, para fins de avaliação do risco, faz-se necessário a observância de determinados critérios pela autoridade competente, quais sejam (§ 1º): (i) natureza dos dados pessoais envolvidos; (ii) finalidades específicas do tratamento; (iii) quantidade de agentes de tratamento de dados envolvidos; (iv) quantidade de titulares de dados potencialmente atingidos; (v) se é utilizado algum tipo de nova tecnologia; (vi) possibilidade de tratamento discriminatório, e as (vii) expectativas legítimas do titular de dados.

A legislação em si, deverá ser instruída com uma análise de impacto regulatório que contenha uma descrição do tratamento e das capacidades da tecnologia de vigilância, os testes ou relatórios relativos aos efeitos do tratamento e da tecnologia de vigilância na saúde e na segurança de pessoas, impactos potencialmente gerados pelo tratamento desses dados em quaisquer populações específicas, as medidas previstas para o surgimento de eventuais riscos, além de garantias, medidas de segurança, mecanismos e política de uso para assegurar a proteção de dados pessoais dos titulares (§2º).

O art. 43 do Anteprojeto veda a utilização dessas tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial, isto é, seria possível a utilização dessas novas tecnologias, no âmbito de atividades de segurança pública, para identificação de pessoas indeterminadas em tempo real, mas esse uso deve ser precedido de autorização legal e judicial, além de ser imprescindível a sua conexão com a investigação criminal desenvolvida.

Ao Conselho Nacional de Justiça também foi direcionada a responsabilidade de emitir opiniões técnicas ou recomendações à utilização de tecnologias de vigilância ou do tratamento de dados pessoais que representem um elevado risco aos direitos e garantias dos titulares, devendo publicar um relatório anual acerca desse uso e realizar uma auditoria nos casos de

descumprimento, sem prejuízo de outros mecanismos de controle e supervisão administrativo e judicial.

Apesar de não haver previsão para implementação e publicação da LGPD Penal, é necessário que o poder legislativo brasileiro se concentre na elaboração célere de legislações específicas que norteiem a implementação dessas novas formas de tecnologia na área de segurança pública e investigação criminal, sob o risco de um aumento exponencial de investigações obsoletas e processos criminais ineficazes, uma vez que o desenvolvimento tecnológico está em nítido e exponencial crescimento.

Para tanto, é imprescindível pensar em uma legislação que não fique caduca diante do desenvolvimento das tecnologias e que disponha de um regime diverso para cada tipo de dado específico (dados pessoais, registros criminais, dados biométricos, dados de localização, entre outros), abordando as suas peculiaridades e pressupostos próprios de legitimação, mas com o cuidado de excesso de juridificação para evitar o engessamento da utilização dessas normas diante de tantos detalhes específicos.

A Convenção de Budapeste em conjunto com a normativa da ABNT NBR ISO/IEC 27037:2012 e o Anteprojeto da LGPD Penal são regulamentos básicos que foram capazes de estipular diretrizes básicas a serem seguidas pelo legislador interno, trazendo temáticas fundamentais para o tratamento da cadeia de custódia, visando garantir a licitude e a credibilidade científica, além de evitar a subjetividade do perito responsável no momento da coleta, tratamento, armazenamento e dispensa da prova digital, e também a própria regulação sobre a proteção de dados, envolvendo o poder estatal e a cooperação internacional para transferência desses dados. Desse modo, o presente estudo pretende demonstrar a relevância e a indispensabilidade de uma futura legislação sobre a utilização e proteção de dados digitais na esfera criminal que possa auxiliar o desenvolvimento de uma segurança pública e de investigações criminais mais eficientes.

5 CONSIDERAÇÕES FINAIS

O avanço da tecnologia no âmbito criminal, especialmente no que se refere à produção e ao uso de dados de geolocalização, impôs novos desafios ao direito probatório no processo penal. Desse modo, a partir da sistematização crítica de decisões judiciais proferidas sobre a temática, do levantamento de dados sobre a ineficiência das investigações quanto à identificação de possíveis autores de crimes realizados pelos participantes do projeto de pesquisa *Criminalidade violenta, justiça criminal e diretrizes para política de segurança pública do estado do Rio Grande do Norte*, e das revisões bibliográficas realizadas ao longo desse estudo, é possível formular as seguintes conclusões.

A colisão entre o direito à intimidade e à privacidade e o direito de proteção (eficiente) por parte do poder público, no âmbito da segurança pública e da investigação criminal, pode ser solucionada a partir da flexibilização dos direitos fundamentais envolvidos, uma vez que a necessidade em resguardar a ordem pública e o exercício policial investigativo se sobrepõe aos interesses particulares dos indivíduos investigados. No entanto, essa flexibilização não deve ser absoluta, mas sim limitada à existência de alguns critérios, como a necessidade de obediência à reserva legal, a existência de uma finalidade vinculada à coleta desses dados e a autorização desse monitoramento através de ordem judicial.

No ambiente criminal, verificou-se o desenvolvimento de novos recursos tecnológicos não só pode servir como fonte de prova para o processo penal, mas são instrumentos indispensáveis diante da complexidade das novas atividades ilícitas. A seara investigativa brasileira encontra ainda mais dificuldades, isso porque os inquéritos policiais ainda são obsoletos quando observada a tecnologia como um instrumento facilitador para as atividades de investigação e repressão de infrações penais. Acontece que muitos desses novos recursos não possuem regulamentação, o que pode dificultar a sua aplicação no processo penal brasileiro.

A garantia da integridade da cadeia de custódia das provas digitais, especialmente os dados de geolocalização, e a proteção aos dados pessoais coletados não possuem, atualmente, normativa que direcione o seu uso e aplicabilidade, sendo necessária a adoção de padrões estabelecidos pela ABNT NBR ISO/IEC 27037:2012 em conjunto com o POP veiculado pela SENASP para que seja possível a produção dessa prova de forma íntegra e legítima, evitando os riscos de serem inutilizadas ou declaradas ilícitas durante a persecução penal.

Por fim, resta evidente que a utilização de ferramentas tecnológicas pode auxiliar em uma maior resolutividade na elucidação dos crimes, especialmente quanto à efetividade na identificação dos responsáveis. No que se refere à utilização do instrumento específico de

geolocalização, percebe-se que a obtenção de dados telemáticos baseados em coordenadas geográficas de usuários que estiveram em locais relevantes é de suma importância para a apuração do fato típico.

No entanto, a ausência de regulamentação específica para o tratamento dessa forma específica de obtenção de dados de localização coloca em risco direitos fundamentais dos indivíduos. O fato de não haver pressupostos peculiares à obtenção de dados de localização previstos em lei, faz com que o Poder Judiciário, na tentativa de resguardar a ordem pública e preservar a efetividade de investigações criminais, profiram decisões judiciais, muitas vezes, genéricas, sem justificação plausível e sem realizar uma delimitação geográfica e temporal razoável em conformidade com a persecução penal.

Assim, é importante a adoção de disciplina jurídica doméstica desenvolvida com base na Convenção de Budapeste em conjunto com a normativa da ABNT NBR ISO/IEC 27037:2012 e o Anteprojeto da LGPD Penal, de modo a contribuir para uma maior efetividade nas áreas de segurança pública e investigação criminal, além de evitar o abuso do poder estatal em detrimento dos indivíduos e o desvirtuamento da medida investigativa com a finalidade de vigilância ou até mesmo perseguição, em nítida desconformidade com a Constituição Federal de 1988 e com a visão garantista do processo penal brasileiro.

REFERÊNCIAS

ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-lgpd. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

ALEXY, Robert. **Constitucionalismo discursivo**. Tradução de Luís Afonso Heck. Porto Alegre: Livraria do advogado, 2007.

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros editores ltda., 2015.

AMARAL, Augusto Jobim do; DIAS, Felipe da Veiga. Surveillance e as "novas" tecnologias de controle biopolítico. ***Veritas***, Porto Alegre, v. 64, n. 1, e-33427, 2019

ARENDT, Hannah. **Origens do totalistarismo**. Tradução de Roberto Raposo. São Paulo: Companhia das letras, 1989.

BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM, ano**, v. 29, p. 7-9, 2021.

BADARÓ, Gustavo Henrique. **Processo Penal**. 9. ed. São Paulo: Thomson Reuters Brasil, 2021.

BARBOSA, Ruy. **A Constituição e os actos inconstitucionais**: do congresso e do executivo ante a justiça federal. 2. ed. Rio de Janeiro: Ataltida Editora, 1893.

BECCARIA, Cesare. **Dos delitos e das penas**. Tradução de J. Cretella Jr. e Agnes Cretella. 2. ed. São Paulo: Editora Revista dos Tribunais, 1999.

BENTHAM, Jeremy; MILLER, Jacques-Alain; PERROT, Michellet; WERRETT, Simon. **O Panóptico**. Tradução de Guacira Lopes Louro, M. D. Magno e Tomaz Tadeu. 2 ed. Belo Horizonte: Autêntica, 2008.

BLAGITZ DE ABREU E SILVA, M. G. Internet e Jurisdição, Acesso Transfronteiriço a Dados e o Caso Irlanda Microsoft. **Revista Eletrônica de Direito Penal e Política Criminal**, *[S. l.]*, v. 5, n. 2, p. 107–117, 2017. Disponível em: https://seer.ufrgs.br/index.php/redppc/article/view/73172. Acesso em: 7 abr. 2023.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 26. ed. Malheiros Editores. São Paulo, 2011.

BRANCO, Paulo Gustavo Gonet; SILVA NETO, Manoel Jorge e; DA MOTA, Helena Mercês Claret; MONTENEGRO, Cristina Rasia; RIBEIRO, Carlos Vinicícius Alves (orgs). **Direitos fundamentais em processo**: estudos em comemoração aos 20 anos da Escola Superior do Ministério Público da União. Brasília: ESMPU, 2020.

BRAZ, José Alberto Campos. **Investigação criminal**. Leya, 2013.

CAPEZ, Fernando. **Curso de processo penal.** São Paulo: Saraiva Educação SA, 2021.

CARNELUTTI, Francesco. **As misérias do processo penal.** Tradução por Carlos Eduardo Trevelin Millan. 2. ed. São Paulo: Editora Pillares, 2009.

CASEY, Eoghan. **Digital evidence and computer crime**: forensic science, computers and the internet. 3 ed. Maryland: Elsevier, 2011.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros – TIC Domicílios 2021.** 2021. Disponível em: https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2021/. Acesso em: 8 abr. 2023.

COHEN, Julie E. What privacy is for. **Harvard Law Review**, v. 126, p. 1904-1933, 2013.

COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. Criminalidade digital no brasil: a problemática e a aplicabilidade da convenção de budapeste. **Revista Em Tempo**, [S.l.], v. 21, n. 1, p. 104-123, aug. 2021.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros**, 2022. Disponível em: https://www.cgi.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2021/. Acesso em: 7 abr. 2023.

CORTEZ, Raphaela Jéssica Reinaldo; SILVA JÚNIOR, Walter Nunes da; GURGEL, Yara Maria Pereira. Dignidade da pessoa humana como instrumento de humanização na execução penal: uma análise da efetividade dos diplomas internacionais no trabalho prisional brasileiro. *In:* MAIA, Catherine; MOREIRA, Thiago Oliveira; GURGEL, Yara Maria Pereira. **Direito Internacional dos Direitos Humanos e as pessoas em situação de vulnerabilidade**. Natal: Polimatia, 2022.

DA SILVA OLIVEIRA, Giuliano; MOREIRA, João Padilha. Internet Via Satélite. **Seminário de tecnologia gestão e educação**, v. 4, n. 2, 2022.

DE ABREU, Melissa Garcia Blagitz. Internet e Jurisdição, Acesso Transfronteiríço a Dados e o Caso Irlanda Microsoft. **Revista Eletrônica de Direito Penal e Política Criminal**, v. 5, n. 2, p. 107-117, 2017.

DE ANDRADE CORDEIRO, Gustavo Henrique; DA FREIRIA ESTEVÃO, Roberto. Garantismo penal integral: o instrumento de proteção suficiente e eficaz dos direitos fundamentais individuais e coletivos. **Novos direitos na contemporaneidade,** v. 1, p. 125, 2021.

DE LIMA, Renato Sérgio; DA SILVA, Guilherme Amorim Campos; DE OLIVEIRA, Priscilla Soares. Segurança Pública e Ordem Pública: apropriação jurídica das expressões à luz da legislação, doutrina e jurisprudência pátrios. **Revista Brasileira de Segurança Pública**, v. 7, n. 1, 2013

DE MIRANDA FONSECA, Idelvandro José; ZAMPOLO, Ronaldo. Análise forense do smartwatch Samsung Galaxy Watch Active 2. **Scientia Plena**, v. 18, n. 8, 2022.

DONAS, Javier Bustamante. Hacia la cuarta generación de Derechos Humanos: repensando la condición humana em la sociedade tecnológica. **CTS+I: Revista ibero-americana de Ciencia, Tecnología, Sociedad e innovación**, v. 1, n.3, 2001.

DONAS, Javier Bustamante. La cuarta generación de derechos humanos em las redes digitales. **Revista TELOS**. p. 1-10, 2010.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

FERRAJOLI, Luigi. **Direito e razão**: teoria do garantismo penal. São Paulo: Editora Revista dos Tribunais, 2002.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito, Universidade de São Paulo**, v. 88, p. 439-459, 1993.

FONSECA, Marcos De Lucca; GENNARINI, Juliana Caramigo. A Adesão do Brasil à Convenção de Budapeste e os Impactos para a Produção de Provas Digitais. **Direito Penal e Processo Penal**, v. 4, n. 1, p. 55-70, 2022.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA**. Anuário Brasileiro de Segurança Pública – 2022**. São Paulo: Fórum brasileiro de segurança pública, 2022. Disponível em: https://forumseguranca.org.br/anuario-brasileiro-seguranca-publica/. Acesso em: 8 abr. 2023.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Raquel Ramalhete. 20 ed. Rio de Janeiro: Vozes, 1999.

GCF GLOBAL. **Histórico de localização do google**: creating opportunities for a better life. Disponível em: https://edu.gcfglobal.org/pt/dicas-tecnologicas/historico-de-localizacao-do-google/1/. Acesso em 20 abr. de 2023.

GREGO, Rogério; BRAGA, Romulo Rhemo Palitot. Da principiologia penal ao direito à intimidade como garantia constitucional. **Revista Direito e Desenvolvimento**, v.2, n.4, p. 142-165, 2012.

GROFF, Paulo Vargas. **Direitos fundamentais nas constituições brasileiras,** Brasília, v. 45, 2008.

GURGEL, Yara Maria Pereira. **Conteúdo normativo da dignidade da pessoa humana e suas implicações jurídicas na realização dos direitos fundamentais**. Tese de Pós-Doutoramento em Direito e Ciências Jurídicas, Universidade de Lisboa, Lisboa, 2018.

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. **BLOQUEIOS.INFO**. Disponível em: https://bloqueios.info/pt/linha-do- tempo/. Acesso em: 22 de abr. 2023.

INSTITUTO SOU DA PAZ**. Onde mora a impunidade?:** Por que o Brasil precisa de um Indicador Nacional de Esclarecimentos de Homicídios. 2022. Disponível em: https://soudapaz.org/o-que-fazemos/conhecer/pesquisas/politicas-de-seguranca-publica/controle-de-homicidios/?show=documentos#6651-1. Acesso em: 8 abr. 2023.

INTERNET WORLD STATS. **World Internet Users and 2023 Population Stats**. 2023. Disponível em: https://www.internetworldstats.com/stats.htm. Acesso em: 8 abr. 2023.

JOELSONS, Marcela *et al*. Inviolabilidade na comunicação dos dados de computador no Brasil versus direito fundamental à confidencialidade e integralidade de sistemas informáticos na Alemanha. **Revista de Direito Constitucional e Internacional**, v. 125, p. 111-135, 2021.

KIST, Dario José. **Prova digital no processo penal**. Leme, SP: JH Mizuno, 2019.

LOPES JÚNIOR, Aury Celso Lima. Vírus espião como meio de investigação: a infiltração por softwares. **Consultor jurídico.** São Paulo: online, 2019

LOPES JÚNIOR, Aury. **Direito processual penal**. 17. ed. São Paulo: Saraiva, 2020.

LOPES JÚNIOR, Aury. **Fundamentos do processo penal**: introdução crítica. 5. ed. São Paulo: Saraiva Educação, 2019.

MACHADO, Javam C.; NETO, Eduardo R. Duarte. Privacidade de Dados de Localização: Modelos, Técnicas e Mecanismos. **Sociedade Brasileira de Computação**, 2021.

MAIA, Tiago Dias; PAULINO, Galtiênio da Cruz. A quebra de sigilo de dados baseada em coordenadas geográficas e o princípio da proporcionalidade. *In:* GONET BRANCO, Paulo Gustavo; SILVA NETO, Manoel Jorge; MOTA, Helena Mercês Claret da; MONTENEGRO, Cristina Rasia; RIBEIRO, Carlos Vinícius Alves (orgs.). **Direitos fundamentais em processo**: estudos em comemoração aos 20 anos da Escola Superior do Ministério Público da União. Brasília: ESMPU, 2020.

MARQUES, Leonardo Augusto Marinho. O Juiz moderno diante da fase de produção de provas: As limitações impostas pela Constituição. **Revista da Faculdade de Direito do Sul de Minas**, v. 24, p. 159-174, 2007.

MEDEIROS, Nathalia Leite de; MARIA DA SILVA, Larissa; CAVALCANTI, Rodrigo; BESSA DA SILVA, Thaise; SILVA SOUSA, Wilde Maxssuaziane da. Os inquéritos policiais relativos aos crimes violentos letais intencionais no estado do Rio Grande do Norte e o dilema da ausência de identificação de autoria. *In*: SILVA JÚNIOR, Walter Nunes da; HAMILTON, Olavo (orgs.). **Política criminal**: monitoramento de espaços públicos, (in)eficiência dos inquéritos policiais, duração razoável dos processos e tratamento dos presos. Natal: OWL, 2022.

MENDES, Gilmar Ferreira. Os Direitos Fundamentais e seus múltiplos significados na ordem constitucional. **Anuário Iberoamericano de Justicia Constitucional**, n. 8, 2004, p. 131-142.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar-Revista de Ciências Jurídicas**, v. 25, n. 4, 2020.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasilera, Lisboa**, v. 5, p. 781-809, 2019.

MINTO, Andressa Olmedo. **A prova digital no processo penal**. São Paulo: LiberArs, 2021.

MONICO, João Francisco Galera. **Posicionamento pelo Navstar-GPS**: descrição, fundamentos e aplicações. São Paulo: Editora UNESP, 2000.

MOREIRA, Thiago Oliveira. **A aplicação dos tratados internacionais de direitos humanos pela jurisdição brasileira**. Natal: EDUFRN, 2015.

NETO, Mário Furlaneto; DOS SANTOS, José Eduardo Lourenço. Apontamentos sobre a cadeia de custódia da prova digital no Brasil. **Revista Em Tempo**, [S.l.], v. 20, n. 1, nov. 2020.

NOVAIS, Jorge Reis. **A dignidade da pessoa humana**. 2. ed. Coimbra: Almedina, 2016. (v.2: Dignidade e Inconstitucionalidade).

NUCCI, Guilherme de Souza. **Direitos humanos versus segurança pública**: questões controvertidas penais, processuais penais, de execução penal e da infância e juventude. Rio de Janeiro: Forense, 2016.

O GLOBO. **Abin de Bolsonaro usou programa secreto para monitorar localização de pessoas por meio do celular**. Disponível em: https://oglobo.globo.com/politica/noticia/2023/03/abin-de-bolsonaro-usou-programa-secreto-para-monitorar-localizacao-de-pessoas-por-meio-do-celular.ghtml. Acesso em 24 abr. de 2023.

PACELLI, Eugênio. **Curso de processo penal**. 22. ed. São Paulo: Atlas ltda., 2017.

PINHEIRO, Patricia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

PINTO, Otoniel Gonçalves. A interceptação telefônica para produção de conhecimento de inteligência. **Homens do Mato-Revista Científica de Pesquisa em Segurança Pública**, v. 16, n. 3, 2017

POSNER, Richard A. The Right to Privacy. **Georgia Law Review**, v. 12, n. 3, 1978.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. São Paulo: Marcial Pons, 2019.

PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**: a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014.

PRADO, Geraldo. Tutela contra a geolocalização contínua. *In:* BRITO CRUZ, Francisco; FRAGOSO, Nathalie. **Direitos fundamentais e processo penal na era digital**: doutrina e prática em debate. São Paulo: InternetLab, 2020. v.3.

RAMOS, André de Carvalho. **Curso de Direitos Humanos**. 6. ed. São Paulo: Saraiva Educação, 2019.

RAZERA, Gustavo Eloi. Acesso a dados criptografados no contexto de investigações criminais: o "estado da arte". **Revista do Ministério Público do Estado do Rio de Janeiro**, v. 79, p. 143, 2021.

REINALDO, Guilherme de Negreiros Diógenes; SILVA JÚNIOR, Walter Nunes da. Estudo de caso sobre a implementação de sistema de videomonitoramento no entorno da sede da Justiça Federal do RN. *In*: SILVA JÚNIOR, Walter Nunes da; HAMILTON, Olavo (orgs.). **Política criminal**: monitoramento de espaços públicos, (in)eficiência dos inquéritos policiais, duração razoável dos processos e tratamento dos presos. Natal: OWL, 2022.

RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. **Revista Brasileira de Direito Processual Penal**, v. 8, p. 1463-1500, 2022.

ROXIN, Claus. Tem futuro o direito penal? **Revista dos Tribunais**, v. 790, p. 459-474, 2001.

SARLET, Ingo Wolfgang. Constituição, proporcionalidade e direitos fundamentais: o direito penal entre proibição de excesso e de insuficiência. **Anuario Iberoamericano de Justicia Constitucional**, n. 10, p. 303-354, 2006.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 4. ed. São Paulo: Saraiva, 2015.

SCHILLER, Jochen; VOISARD, Agnès (Ed.). **Location-based services**. Elsevier, 2004.

SILVA JÚNIOR, Walter Nunes da. **Curso de Direito Processual Penal**: Teoria (Constitucional) do Processo Penal. 3. ed. Natal: OWL, 2021.

SILVA JÚNIOR, Walter Nunes da. **Reforma tópica do processo penal**: inovações aos procedimentos ordinário e sumário, com o novo regime das provas, principais modificações do júri e as medidas cautelares pessoais (prisão e medidas diversas da prisão). 4. ed. Natal: OWL, 2022.

SILVA, Virgílio Afonso da. **Direitos fundamentais:** conteúdo essencial, restrições e eficácia. 2. ed. São Paulo: Malheiros, 2017.

SMANIO, Gianluca Martins. A busca reversa por dados de localização na jurisprudência do Superior Tribunal de Justiça: análise crítica do RMS 61.302/RJ. **Revista Brasileira de Ciências Policiais**, v. 12, n. 5, p. 49-76, 2021.

SOUZA, Gabriel Lucas Moura; FREIRE, Natália Galvão da Cunha Lima. A cadeia de custódia da prova e sua (in)eficiência diante da desvalorização da forma processual. *In*: **Pacote anticrime:** temas relevantes. Natal: OWL, 2020.

TERRA JÚNIOR, João Santa. A Utilização Da Interceptação Telefônica No Combate À Criminalidade Atual. **Artigo Científico**, p. 01, 2003.

TOMAÉL, Maria Inês; ALCARÁ, Adriana Rosecler; DI CHIARA, Ivone Guerreiro. Das redes sociais à inovação. **Ciência da informação**, v. 34, p. 93-104, 2005

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, p. 269-285, 2016.

TORRES, Ricardo Lobo. **O direito ao mínimo existencial**. Rio de Janeiro: Renovar, 2009.

VAZ, Denise Provasi. **Provas digitais no processo penal**: formulação do conceito, definição das características e sistematização do procedimento probatório. Tese (Doutorado) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012.

VERASZTO, Estéfano Vizconde, DA SILVA, Dirceu, MIRANDA, Nonato Assis, SIMON, Fernanda Oliveira. Tecnologia: buscando uma definição para o conceito. **Prisma.com**, n. 8, p. 19-46, 2009.

WARREN, Samuel D.; BRANDEIS, Luis D. The Right to Privacy. **Harvard Law Review**, v. 4, dec. 15, 1890.

ZAFFARONI, Eugenio Raúl. La influencia del pensamento de Cesare Beccaria sobre la política criminal en el mundo. **Anuario de derecho penal y ciências penales**, p. 521-552, 1989.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira de poder. Tradução de George Schlosinger. Rio de Janeiro: Intrínseca, 2021.