A QUEBRA DE SIGILO DE DADOS TELEMÁTICOS EM CASOS DE INVESTIGAÇÃO CRIMINAL: UMA REFLEXÃO SOBRE O USO DE DADOS ELETRÔNICOS COMO PROVA NO PROCESSO PENAL

SILVA, Israel Martimiano da[1]
SILVA JR, José Roberto Martins da[2]

RESUMO: A quebra do sigilo telemático de dados é uma prática essencial nas investigações criminais, permitindo que as autoridades tenham acesso a informações digitais relevantes para solucionar crimes. Essa quebra de confidencialidade refere-se à aquisição legal de dados eletrônicos protegidos por medidas de segurança ou privacidade. Os dados telemáticos incluem uma variedade de informações, como registros de comunicação, histórico de navegação na *web*, dados de localização e arquivos armazenados em dispositivos eletrônicos. Para concretizar a violação do sigilo dos dados telemáticos, as autoridades geralmente obtêm mandados judiciais específicos que autorizam o acesso a essas informações. Os métodos utilizados podem variar, incluindo extração forense de dispositivos eletrônicos, solicitação de registros de provedores de serviços de Internet e utilização de técnicas avançadas de análise de dados. No entanto, esse processo levanta questões de privacidade e direitos individuais. A obtenção de dados telemáticos envolve, frequentemente, o recolhimento de informações pessoais sensíveis, levantando preocupações sobre potenciais abusos de poder por parte das autoridades. Portanto, é crucial que os procedimentos de quebra de confidencialidade sejam conduzidos de acordo com a legislação aplicável e respeitando os direitos fundamentais dos indivíduos. Além disso, a rápida evolução da tecnologia apresenta desafios adicionais para as investigações, exigindo que os investigadores se mantenham atualizados com as mais recentes técnicas e ferramentas forenses digitais.

PALAVRAS-CHAVE: Dados, Sigilo, Investigação.

THE DISCLOSURE OF TELEMATIC DATA PRIVACY IN CRIMINAL INVESTIGATIONS: A REFLECTION ON THE USE OF ELECTRONIC DATA AS EVIDENCE IN CRIMINAL PROCEEDINGS

ABSTRACT: The breach of telematic data confidentiality is an essential practice in criminal investigations, allowing authorities to access relevant digital information to solve crimes. This breach of confidentiality refers to the legal acquisition of electronic data protected by security or privacy measures. Telematic data includes a variety of information, such as communication records, web browsing history, location data, and files stored on electronic devices. To carry out the breach of telematic data confidentiality, authorities generally obtain specific judicial warrants authorizing access to this information. The methods used may vary, including forensic extraction of electronic devices, requesting records from internet service providers, and utilizing advanced data analysis techniques. However, this process raises privacy and individual rights issues. Obtaining telematic data often involves collecting sensitive personal information, raising concerns about potential abuse of power by authorities. Therefore, it is crucial that confidentiality breach procedures be conducted in accordance with applicable legislation and respect for individuals' fundamental rights. Additionally, the rapid evolution of technology presents additional challenges for investigations, requiring investigators to stay updated with the latest digital forensic techniques and tools.

KEYWORS: Data, Secrecy, Investigation.

[1] Acadêmico do Curso de Direito do Centro Universitário FAG. E-mail: imsilva2@minha.fag.edu.br.
[2] Mestre em Ciências Ambientais pela Universidade Estadual do Oeste do Paraná – UNIOESTE, Docente Orientador do Curso de Direito do Centro Universitário FAG. E-mail: josejr@fag.edu.br.

1 INTRODUÇÃO

O foco deste trabalho versa sobre a divulgação de informações telemáticas em contextos de investigação criminal, abordando não apenas a questão do seu uso excessivo, mas também os impactos negativos que podem afetar terceiros, resultando na violação de seus direitos fundamentais.

O tema escolhido trata das violações do sigilo dos dados telemáticos nas investigações criminais e aborda um assunto contemporâneo e que ocorre com demasiada frequência. Diz respeito à salvaguarda da privacidade, intimidade e proteção da comunicação e à utilização de dados eletrônicos com vista às investigações em processos penais. Além disso, o tema também suscita debates sobre os conceitos de prova e os meios para obtê-la, bem como sobre a validade de princípios, como o contraditório, a ampla defesa e o devido processo legal. Sabemos que a violação de dados telemáticos (telefônicos e informáticos) se tornou uma realidade com a Lei n° 9.296/96, que passou a regulamentar o inciso XII do artigo 5º da Constituição Federal de 1988, que trata da inviolabilidade do sigilo das comunicações, salvo no âmbito de investigações criminais e formações de processo.

No entanto, ao falar sobre os custos de uma violação de dados, é extremamente importante salientar que os investigadores não são comunicados apenas sobre o suposto objeto da investigação, mas também sobre dados pessoais, como fotos, vídeos, mensagens de trabalho ou a privacidade do indivíduo, bem como as mesmas informações no âmbito de terceiros que, mesmo não sendo objeto da investigação, são finalmente divulgadas, sem direito de contraditório ou à defesa completa, nomeadamente sem direito de suspensão ou atenuação de seus direitos.

No mesmo sentido, cabe destacar que, além da exposição dos dados que existem sobre o investigado e as pessoas ao seu redor durante uma investigação, é preciso lembrar que, quase sempre, os dispositivos telemáticos em posse de registros policiais são ferramentas de trabalho do investigado, como computadores e celulares, que muitas vezes ficam em poder da polícia por mesesou anos.

Portanto, oferecer uma discussão remota sobre violação de privacidade é essencial, relevante e oportuno, já que recentemente foram publicadas muitas notícias sobre violação de privacidade. É importante compreender a razoabilidade de promover a "mitigação" da privacidade, do sigilo e da intimidade para a obtenção de informações relevantes para o Processo Penal.

A problemática deste artigo se dá por meio dos questionamentos: Quais são os

desafios éticos e legais associados à coleta e ao armazenamento de dados telemáticos para fins de investigação criminal? Como garantir a integridade e a segurança desses dados? E no que tange à legislação e à regulamentação, quais são as leis e os regulamentos atuais relacionados à quebra de sigilo de dados telemáticos em investigações criminais? Eles são suficientes para lidar com os desafios contemporâneos, como a criptografia e as redes sociais?

Em relação à coleta e ao armazenamento de dados telemáticos para fins de investigação criminal,é imperativo que haja uma implementação de políticas de governança de dados mais rigorosas e transparentes, com o fim de estabelecer regulamentações claras e abrangentes que definam os procedimentos para a coleta, o armazenamento, o uso e o compartilhamento de dados telemáticos em investigações criminais. Essas regulamentações devem garantir a proteção dos direitos individuais e a conformidade com os princípios éticos.

Considerando a necessidade de existirem padrões de segurança robustos, necessária se faz a implementação de medidas de segurança de dados robustas para proteger a integridade e a confidencialidade das informações coletadas. Isso pode incluir criptografia de ponta a ponta, controle de acesso rigoroso e proteção contra ataques cibernéticos.

No mesmo sentido, precisamos de mais transparência, como, por exemplo, prestação de contas por parte das autoridades de aplicação da lei sobre os processos de coleta e armazenamento de dados telemáticos, incluindo a divulgação de informações sobre os tipos de dados coletados, os fins para os quais são usados e os prazos de retenção. Além disso, é imprescindível estabelecer mecanismos eficazes de prestação de contas para garantir que o uso dos dados seja legal, ético e justificado.

Também se faz necessário promover a educação e a conscientização pública sobre questões relacionadas à coleta e ao armazenamento de dados telemáticos, destacando os direitos individuais dos cidadãos e as medidas de proteção disponíveis. Isso pode ajudar a construir confiança entre o público e as autoridades de aplicação da lei, facilitando a cooperação e o apoio às investigações criminais.

No que tange à legislação e à regulamentação, para lidar com os deságios contemporâneos, como a criptografia e as redes sociais, uma solução viável seria uma abordagem multidisciplinar que envolvesse a atualização da legislação, colaboração entre especialistas, adoção de abordagens flexíveis e cooperação internacional, conforme discorreremos a seguir.

Sobre a atualização da legislação, faz-se necessário rever e atualizar regularmente as leis e regulamentos relacionados à quebra de sigilo de dados telemáticos para garantir que sejam adequados para lidar com os avanços tecnológicos e os novos desafios enfrentados pelas autoridades de aplicação da lei. Isso pode incluir a introdução de emendas específicas para abordar questões como criptografia, proteção de dados pessoais e cooperação internacional em investigações criminais.

No mesmo contexto, o tema carece de colaboração entre especialistas, desse modo incumbe ao poder público promover a colaboração entre legisladores, especialistas em tecnologia, profissionais jurídicos, representantes da sociedade civil e outras partes interessadas para desenvolver políticas e regulamentos eficazes que equilibrem as necessidades de segurança pública e os direitos individuais à privacidade.

Ainda discorrendo sobre colaboração, o tema muitas das vezes traspassa as fronteiras do Brasil. Dessa forma, é interessante ao País fortalecer a cooperação internacional e a harmonização das leis e regulamentos entre os países para facilitar a investigação transfronteiriça de crimes cibernéticos e garantir que os investigadores tenham acesso efetivo aos dados telemáticos, respeitando ao mesmo tempo os princípios de soberania nacional e os direitos individuais.

Por fim, também é importante adotar abordagens flexíveis que possam se adaptar às mudanças rápidas no cenário tecnológico, permitindo que a legislação e a regulamentação sejam ajustadas conforme necessário para lidar com novos desafios e oportunidades.

A pesquisa tem como objetivo oferecer uma análise abordando a divulgação de informações telemáticas, abordando as leis aplicáveis e a orientação dos tribunais em relação a esse tópico. Ela busca ilustrar a maneira pela qual esses dados são empregados como evidência no contexto do sistema de justiça penal do Brasil.

Mais especificadamente, este trabalho tem ainda o fito de apresentar breves considerações sobre alguns princípios essenciais do Processo Penal, tais como: a ampla defesa, o contraditório e o devido processo legal e, dessa forma, discorrer ainda sobre a intimidade e a privacidade na Constituição Federal de 1988, conceituar provas, entender seu limites e formas de obtenção e, por fim, analisar as disposições legais e o posicionamento dos Tribunais Superiores quanto ao sigilo e utilização de dados telemáticos no Processo Penal.

2 DAS PROVAS NO PROCESSO PENAL

As provas no Direito Processual Penal constituem um dos assuntos mais relevantes da disciplina, uma vez que servem de motivação à sentença judicial. Provas capazes de refletir a realidade da forma mais aproximada à realidade dos fatos têm uma possibilidade maior de resultar em sentenças justas. Dessa forma, frisa-se que a realidade dos fatos não reside em uma busca da verdade a qualquer custo, pois essa postura desrespeita direitos e garantias fundamentais, em especial as do acusado no processo criminal (Fernandes, 2011).

O tema da prova no processo recebe especial destaque considerando que, em um passado recente, predominava como entendimento no processo penal o princípio da verdade material, acreditando-se na possibilidade da reprodução exata do fato ocorrido em todas as suas versões, por meio da produção probatória. Ocorre que a verdade material é inalcançável, restando apenas a verdade processual, por ser entendida como possível de ser atingida (Fernandes, 2011).

No que tange à fonte de prova, aos meios de produção de prova e aos meios empregados para a investigação da prova, observa-se que fonte de prova pode ser definida como coisas ou pessoas pelas quais é possível obter uma prova, surgindo dessa forma a seguinte classificação: fontes testemunhais e fontes documentais (Fernandes, 2011).

Os meios de prova, conhecidos também como meios de produção de prova, referem-se aos instrumentos ou atividades utilizados para introduzir e registrar os dados probatórios no processo. Já os meios de investigação da prova, ou de pesquisa da prova, são o conjunto de procedimentos empregados e regulados por lei, com o fito em adquirir elementos materiais. Os referidos procedimentos são realizados por servidores públicos, como, por exemplo, os policiais ou peritos (Fernandes, 2011).

2.1 DO DIREITO CONSTITUCIONAL À PRIVACIDADE, À INTIMIDADE E À VIDA PRIVADA

A Constituição Federal Brasileira de 1988, em seu artigo 5º, inciso X, dispõe que a privacidade é um direito fundamental e, por tanto, é inviolável (Brasil, 1988). Esse direito abrange as relações de amizade e familiares, protegendo-as do mundo exterior por meio do domicílio. O Direito intervém nessas relações para preservá-las e fortalecê-las, destacando desse modo, a privacidade e a vida privada como o cerne do espaço privado. Dessa forma, o espaço estritamente privado do indivíduo abriga sua pessoalidade e intimidade, juntamente

com sua família, protegida pelo domicílio. Esse ambiente não é reservado, pertencendo ao sujeito em contraste com a sociedade, com o objetivo de satisfazer seus interesses privados, individuais e coletivos (Barroso, 2016).

Assim sendo, esse direito busca proteger o cidadão contra a interferência em sua intimidade, bem como a ingerência de sua integridade física ou mental, sua moralidade e liberdade de pensamento, além de sua honra e fama, a intervenção na correspondência e a transmissão de dados pessoais ou recebidos em razão de segredo profissional (Moraes, 2016).

Nesse sentido, também consta na Constituição Federal, no artigo 5º, inciso XII, que dispõe sobre a inviolabilidade do sigilo das comunicações telefônicas e telegráficas, porém, exceto nas hipóteses de instrução para o processo penal ou ordem judicial para fins de investigação criminal (Moraes, 2016). Ainda, o direito à intimidade encontra-se consagrado, além da Constituição Federal brasileira, na Declaração Universal dos Direitos Humanos, em seu artigo XII, ao afirmar que ninguém será sujeito a interferências de sua vida privada (Greco, 2015).

Alexandre de Moraes, em sua obra *Direito Constitucional*, define e diferencia o direito à privacidade e à intimidade, afirmando que a intimidade se funda nas relações subjetivas e de trato íntimo da pessoa. Exemplo disso é a relação com familiares e amigos. Já o direito à privacidade envolve todos os demais pontos dos relacionamentos humanos, como relações de negócios, laborativas ou de estudo (Moraes, 2016).

Ainda, é inviolável o sigilo das comunicações telegráficas, bem como da correspondência e de dados e das comunicações telefônicas, tendo por exceção a essa regra os casos em que houver ordem judicial em conformidade com a forma em que é estabelecida na lei para fins de instrução processual penal ou até mesmo, de investigação criminal. A exceção exposta pela Constituição menciona que, com a interceptação telefônica, é compreendido que nenhuma liberdade individual ou direito fundamental é absoluto, havendo a possibilidade da interceptação sempre que as liberdades públicas utilizem como instrumento de proteção de práticas ilegais (Moraes, 2016).

2.2 O PROCEDIMENTO DA INTERCEPTAÇÃO DE COMUNICAÇÕES TELEFÔNICAS

De acordo com o artigo 156 do CPP, de modo geral, o ônus de provar aquilo que é alegado, é daquele que o fizer, no caso, do acusador. Isso decorre do princípio da presunção de inocência. Ocorre que o juiz também se utiliza de ferramentas de instrução processual

penal, para determinar a produção de provas sem que haja a provocação para tanto pelas partes. Tal poder decorre de sua faculdade de ordenar, e isso pode ocorrer mesmo na fase de investigação, quando essa produção probatória tem caráter urgente (Minto, 2021).

A produção probatória pode significar a personificação do desejo da parte em refutar ou refutar o fato que é indispensável à solução razoável do caso penal. Tratando do processo penal em um modelo ideal em que se impera a imparcialidade do julgador, a produção das provas é ato privativo das partes, e somente de forma excepcional e em caráter substitutivo, esse ônus deve incumbir à autoridade judicial. Dessa forma, para justificar o abandono da inércia, a necessidade de atuação do juiz deve ser insuperável, como, por exemplo, nas hipóteses em que se faz necessário afastar uma garantia individual para a produção probatória, como é o caso da interceptação de conversas telefônicas (Minto, 2021).

Nesse sentido, o art. 5º da Constituição Federal de 1988 determina a inviolabilidade das comunicações telegráficas, do sigilo da correspondência e das comunicações telefônicas, trazendo uma exceção, que ocorre quando por ordem judicial, e para investigações criminais. Esse meio de aquisição de prova está previsto na legislação interna e tem por finalidade interceptar as comunicações telemáticas para encontrar evidências da prática de algum delito (Minto, 2021).

Ocorre que esse é um meio de prova excepcional, já que a Lei n° 9.296/96 impõe diversos requisitos para sua aplicação, como, por exemplo, a adoção de tal medida apenas quando ocorrerem indícios razoáveis da autoria ou participação em algum crime, em que a prova não puder ser feita por outros meios disponíveis, bem como o fato investigado constituir infração penal punida no máximo com pena de detenção (Minto, 2021).

Sendo assim, conforme a necessidade, a fim de consolidar os elementos úteis para que o Ministério Público ofereça a ação penal, poderá a autoridade policial requisitar ao juiz a realização de medidas restritivas de direitos, isto é, a realização de escutas telefônicas, por exemplo (Lopes, 2019).

Porém, a exigência de investigação criminal não exige a prévia abertura de inquérito policial, necessitando apenas que o Ministério Público compreenda, por necessário, a produção desta prova para assim possibilitar a formação de seu convencimento ao longo do procedimento da investigação criminal preliminar (Moraes, 2016).

Contudo, ao não cumprir os requisitos exigidos para o procedimento da interceptação telefônica, isto é, ela ser ilegal, e dela prova ilegal virem à tona novos fatos, nada poderá ser feito em razão do princípio da contaminação, que determina que o vício ocorrido em um ato é transmitido a todos os atos seguintes que possuem sua gênese no ato viciado. Exemplo

disso é a apreensão de objetos usados na prática de um crime, e que essa informação tenha sido alcançada a partir de uma escuta telefônica ilegal ou por meio de violação de correspondência eletrônica sem a devida permissão. Assim, mesmo que a busca e apreensão ocorram de forma correta, é um ato derivado de um ato ilícito. Portanto, é viciado (Lopes, 2019).

No decorrer do procedimento legal, o juiz tem a prerrogativa de optar por uma das modalidades de interceptação telefônica, conforme descritas por Capez: a) interceptação telefônica refere-se à gravação de uma conversa por um terceiro, sem o consentimento dos interlocutores; b) escuta telefônica é a gravação de uma conversa com o consentimento de um dos interlocutores; c) interceptação ambiental envolve a gravação de uma conversa entre pessoas presentes, realizada por um terceiro no mesmo ambiente dos interlocutores, mas sem o consentimento destes; d) escuta ambiental é a gravação de uma conversa entre pessoas presentes por um terceiro, com o consentimento de um ou mais presentes; e) gravação clandestina é realizada pelo próprio interlocutor ao gravar sua conversa com terceiros, sem o consentimento destes (Capez, 2016).

Desse modo, a produção desta prova é conduzida pela autoridade policial, por meio da requisição aos serviços de telecomunicações, com prévia anuência do Ministério Público. Feito isso, a prova adquirida permanecerá em segredo de justiça, devendo assim, caso exista ação penal em curso, ser possibilitado ao defensor a análise, respeitando o princípio do devido processo legal (Moraes, 2016).

Porém, na hipótese de a quebra de sigilo telefônico atingir terceiros, o produto dessa interceptação telefônica não pode ser utilizado, pois viola a especialidade e vinculação da prova, sendo isso um debate, não existindo pacificação jurisprudencial nesse tema (Lopes, 2019).

2.3 A LEI CAROLINA DIECKMANN

Em 2012, no Brasil, houve duas leis de grande relevância ao combate as novas formas de cometimento de crimes na internet, a Lei n° 12.737, de 2012, popularmente denominada Lei Carolina Dieckmann, e a Lei n° 12.735 de 2012, conhecida como Lei Azeredo (Brasil, 2012). Ambas as leis tiveram uma grande importância para o combate aos crimes digitais.

A Lei n° 12.735 de 2012 trouxe apenas duas disposições normativas, a primeira se refere a uma determinação para as autoridades policiais sobre uma estruturação organizada

para um combate aos crimes digitais mais eficaz, enquanto a segunda traz a hipótese de cessação de transmissões digitais quando houver o cometimento de induzimento ou incitação ao preconceito ou discriminação de raça, cor, etnia, religião ou procedência nacional (Alves, 2020).

Já a Lei n° 12.737 teve origem após a notícia de repercussão nacional, com o vazamento de fotos íntimas da atriz Carolina Dieckmann na internet, tendo assim uma forte influência midiática, o que não é o ideal no processo legislativo, pois os assuntos não são debatidos com a seriedade que se espera (Alves, 2020).

No que diz respeito à legislação, ela inclui disposições no Código Penal Brasileiro, que abordam os crimes de invasão de dispositivos informáticos, conhecidos também como intrusão informática, tipificados pelo artigo 154-A, interrupção ou perturbação de serviços de comunicação telegráfica, telefônica, informática, telemática ou de informação de interesse público (artigo 266) e falsificação de cartões (artigo 298, parágrafo único) (Alves, 2020).

O crime de instrução informática, previsto no Código Penal, em seu artigo 154-A, pode ocorrer por diversas razões, tais como pelo mero desafio de superar a segurança e invadir a privacidade alheia ou, nos piores casos, na intenção de manipular ou sabotar informações e dados, e com isso se tornando um crime meio para a prática de diversos outros crimes. Ocorre que ainda ficou uma grande insegurança jurídica, pois o legislador decidiu não tipificar as demais condutas e nem sequer aduzir formas mais específicas para o seu enfrentamento (Alves, 2020).

2.4 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD) não visa à defesa dos dados das empresas, mas sim dos dados das pessoas que estão sob o tratamento das empresas, isto é, dos dados das pessoas físicas, sejam elas terceiros, funcionários, acionistas ou clientes, ou seja, visa à proteção dos dados de todos. O que faz a LGPD ter principal relevância dentre todos os diapositivos legais já tratados sobre o tema é a sua capacidade de inovar ao criar sanções direcionadas, bem como sobre a nova governança que adiciona um novo órgão da Presidência da República (Garcia, et al. 2020).

A Lei Geral de Proteção de Dados (LGPD), Lei n° 13.709/2018, vai além de simples diretrizes ou regulamentos; ela estabelece direitos, princípios e responsabilidades para o uso de dados pessoais, desempenhando um papel crucial na sociedade

contemporânea. Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) foi instituída como um órgão governamental com a missão de proteger e garantir a implementação da LGPD em todo o território nacional. A ANPD é encarregada de supervisionar o cumprimento da legislação e de aplicar sanções em casos de violação da LGPD (Pinheiro, 2021).

Contando com 11 capítulos e 65 artigos, a Lei Geral de Proteção de Dados (LGPD) foi concebida com o intuito de conceder maior autonomia e reforçar a salvaguarda da privacidade das pessoas às quais os dados pertencem. O respeito, a garantia da segurança e a transparência para o usuário foram os princípios fundamentais que orientaram as disposições regulatórias. Delegar responsabilidades de monitoramento e fiscalização a profissionais que não considerem a perspectiva do indivíduo pode resultar em decisões conflitantes e que se distanciam dos objetivos da legislação (Pinheiro, 2021).

De modo geral, a LGPD estabelece direitos para os titulares de dados, como acesso à informação, correção de dados, exclusão de dados e revogação do consentimento. Ela também define as ações e responsabilidades dos agentes de tratamento de dados, que devem realizar o tratamento de acordo com a finalidade e adequação necessárias, cientes de que o descumprimento acarreta sanções que incluem advertências, multas de até 2% do faturamento com limite de R$ 50 milhões por infração, multas diárias, bloqueio e exclusão dos dados, podendo chegar até à proibição total das atividades relacionadas ao tratamento de dados pessoais (Pinheiro, 2021).

Além disso, a LGPD estabelece condições básicas para o tratamento legítimo de dados, como consentimento informado do titular, finalidade clara e específica, acesso à informação, minimização dos dados coletados, transparência nas ações e garantias de segurança e privacidade dos dados (Pinheiro, 2021).

Dessa forma, fica evidente que a LGPD é uma lei complexa e de alto impacto, por estabelecer uma série de procedimentos específicos, além de reafirmar princípios que já estavam presentes em outras leis, como, por exemplo, a Constituição Federal de 1988 e o Marco Civil da Internet.

2.5 O MARCO CIVIL DA INTERNET E SUAS NOVIDADES PARA O DIREITO DIGITAL

O Projeto de Lei nº 2126 foi transformado na Lei nº 12.965 após quase três anos de processo legislativo. Mais conhecida como Marco Civil da Internet, essa lei foi promulgada

em 23 de abril de 2014. Ela estabelece direitos, deveres e garantias para o uso da internet no Brasil, definindo normas a serem seguidas pela União, pelos Estados, pelo Distrito Federal e pelos Municípios em relação a esse tema (Brasil,2014).

Em um primeiro momento, na visão do legislador, a internet no Brasil tem caráter de um direito difuso e universal, por força de seu artigo 4º, inciso I, ao determinar que seu acesso é direito de todos. Com a vigência do Marco Civil da Internet, as empresas que atuam na internet passam a operar de forma mais transparente, a proteção da privacidade dos usuários e de seus dados pessoais se torna objeto de proteção legal e garantida por lei (Alves, 2020).

E com essa maior proteção dos dados dos usuários, a sua proteção só pode ser quebrada por meio de ordem judicial. Isso também significa que, caso o internauta deseje encerrar sua conta em uma rede social, ou em algum serviço online, este pode requerer que seus dados pessoais sejam deletados definitivamente, pois com o Marco Civil da Internet agora é garantido que os dados das pessoas pertençam a elas mesmas, e não a terceiros (Alves, 2020).

Outra novidade é a asseguração da privacidade das comunicações, que anteriormente era limitada e não se aplicava aos serviços de e-mail, por exemplo. A partir desse momento, o conteúdo das comunicações privadas em meios eletrônicos passa a receber a mesma proteção de privacidade que já era estabelecida para os meios de comunicação convencionais, como cartas e conversas telefônicas (Alves, 2020).

Quanto ao procedimento das investigações policiais, Spencer Toth Sydow destaca a necessidade de distinguir entre os conceitos de "dados estáticos" e "dados dinâmicos". Os dados estáticos referem-se aos registros fixos que um usuário possui na rede, enquanto os dados dinâmicos englobam informações como histórico de navegação, conversas e registros de downloads.

Para acessar os dados estáticos, o inciso IV do artigo 3º da Lei nº 12.850 de 2013, a Lei de Organização Criminosa, comumente conhecida por esse nome, estabelece que, em qualquer etapa do processo penal, são autorizados métodos para obtenção de evidências, incluindo "acesso a registros de chamadas telefônicas e telemáticas, a dados cadastrais armazenados em bancos de dados públicos ou privados, bem como a informações eleitorais ou comerciais" (Brasil, 2013).

Já para os dados dinâmicos, a regulamentação é estabelecida pelo Marco Civil da Internet, que determina que tais dados só possam ser fornecidos mediante autorização judicial (Sydow, 2015).

Uma das mudanças mais relevantes trazidas com o advento do Marco Civil da Internet é a retirada de conteúdos impróprios do ar, afinal, antes de sua promulgação, não existia nenhuma norma clara sobre o procedimento. Sendo assim, a retirada desses conteúdos passou a ser executada mediante ordem judicial, em exceção dos casos de "pornografia de vingança", do qual a própria vítima poderá solicitar a retirada do conteúdo diretamente dos sites ou serviços em que esses conteúdos estejam hospedados (Alves, 2020).

Em resumo, conforme observado por Sydow, embora essa legislação apresente várias falhas, ela desempenha um papel crucial no campo do Direito Penal, relacionado à informática e aos crimes digitais (Sydow, et al. 2015), pois contribui de maneira substancial para uma interpretação apropriada e tenta abordar algumas das questões em aberto sobre o tema.

2.6 DA CONVENÇÃO DE BUDAPESTE NO BRASIL E DOS MEIOS DE OBTENÇÃO DE PROVA DIGITAL

Por meio do Decreto n° 11.491, de 12 de abril de 2023, foi promulgada a Convenção sobre o Crime Cibernético, que foi firmado pelo Brasil em Budapeste, na data de 23 de novembro de 2001. Essa lei estabelece regramentos gerais para a obtenção de provas. Dentre os seus institutos, temos a busca e apreensão de dados informáticos armazenados, a recolha em tempo real de dados informáticos, a injunção e a conservação expedita de dados informáticos armazenados (Brasil, 2023).

A conservação expedita de dados informáticos armazenados refere-se à prática de manter registros de informações digitais por um período determinado de tempo para diversos fins, como investigações criminais, proteção de dados pessoais, conformidade regulatória, entre outros. Esses dados informáticos podem incluir registros de comunicações eletrônicas (como e-mails, mensagens instantâneas), registros de acesso a sistemas e redes, registros de transações financeiras, entre outros tipos de dados digitais (Brasil, 2023).

O artigo 18 da Convenção de Budapeste permite que os Estados signatários adotem medidas legislativas que permitam às autoridades ordenar que indivíduos ou entidades que detenham dados informáticos específicos os apresentem ou concedam acesso a eles, assim denominada, a injunção. É importante ressaltar que essa medida não se destina à conservação de dados, como ocorre com a conservação expedita, mas sim à apreensão ou acesso aos dados. Dessa forma, a sua utilidade reside no fato de permitir o acesso desses

dados pelas autoridades, auxiliando nas investigações criminais com a colaboração do detentor dos dados (Minto, 2021).

Embora existam outros métodos de acesso aos dados, como busca e apreensão, a capacidade de ocultar informações ou bloquear o acesso a elas pode dificultar o sucesso dessas diligências. O destinatário da ordem pode ser qualquer pessoa física ou jurídica que tenha posse ou controle sobre os dados, exceto o investigado, em respeito ao princípio *nemo tenetur se detegere*, que garante o direito de não produzir provas contra si mesmo (Minto, 2021).

A busca e apreensão de dados informáticos armazenados é um método para a obtenção de provas digitais que está previsto no artigo 19 da Convenção de Budapeste. Esse artigo estipula que os Estados signatários devem adotar medidas legislativas para capacitar suas autoridades competentes a realizar buscas em: a) sistemas informáticos ou partes deles, assim como nos dados armazenados neles; b) dispositivos de armazenamento de dados informáticos (Minto, 2021).

Nesse tipo de obtenção de prova, o Estado possui as seguintes prerrogativas: a) apreender ou obter o sistema informático ou parte dele, assim como o dispositivo de armazenamento dos dados informáticos; b) fazer e manter uma cópia desses dados informáticos; c) preservar a integridade dos dados armazenados; d) tornar os dados inacessíveis ou removê-los do sistema informático armazenado. Dessa forma, esse método de obtenção de prova não tem o objetivo de conservar dados nem de solicitar acesso à pessoa que os detém, mas sim de buscá-los e apreendê-los sem qualquer comunicação prévia com o detentor (Minto, 2021).

Os artigos 20 e 21 da Convenção de Budapeste abordam a interceptação de dados informáticos durante sua transmissão, diferenciando-se da busca de dados já armazenados ao focar em comunicações em tempo real. Esses meios específicos de obtenção de provas digitais são vitais devido à crescente utilização de sistemas informáticos em diversas atividades criminosas, aproveitando sua capacidade de transmitir dados de formas variadas e a possibilidade de manipulação ou eliminação das evidências digitais. Em geral, somente especialistas em Ciência Forense Digital possuem o conhecimento necessário para avaliar adequadamente essas evidências e compreender suas particularidades (Minto, 2021).

Dessa forma, fica evidente que a adoção do Brasil pela respectiva convenção internacional representa um avanço legislativo significativo que estabelece regramentos para a investigação digital no País, regulamentando atos de entes e agentes públicos no interesse estatal de elucidar crimes e promover a justiça.

2.7 DA LICITUDE DA PRODUÇÃO DA PROVA

Para a quebra de sigilo de dados telefônicos entende-se que a Lei se refere aos dados armazenados nas empresas de telefonia, sendo necessária a autorização judicial para a obtenção de conversas telefônicas em andamento. Porém, os registros de ligações já realizadas são documentos normais, logo, não necessitam do procedimento para ser requisitados ao juiz (Capez, 2016).

Diante disso, no caso de ser realizada uma das provas acima citadas, contudo, em desacordo com as exigências dos procedimentos, por exemplo, ser efetuada a interceptação telefônica sem a autorização por meio da decisão judicial, esta se constitui em prova ilegal, sendo aquela que viola o direito material ou a Constituição na sua realização ou no mesmo tempo ao processo, porém, sempre externo a este. Assim, ocorre a violação da intimidade, privacidade ou dignidade, sendo um exemplo de prova ilegal a interceptação telefônica viciada (Lopes, 2019).

Desse modo, as provas adquiridas por meio de meios ilícitos não podem ser admitidas, sendo vedadas conforme artigo 5º, inciso LVI, da Constituição Federal, em razão de ser uma garantia aos sujeitos em relação a perseguições praticadas pelo Estado, por isso, não se permite a realização de prova ilegal (Moraes, 2016).

Em consonância com o exposto, a prova obtida por meio de afronta às regras de direito material, o que a torna ilegal, não é permitida em nenhum tipo de processo em razão de sua vedação na Constituição Federal bem como no Código de Processo Penal (Capez, 2019).

Assim, na hipótese de a interceptação telefônica ser realizada de forma ilícita, ela é considerada inadmissível conforme expresso na Constituição em seu artigo 5º, inciso LVI. A legislação estabelece que as provas obtidas por meios ilícitos são consideradas "inadmissíveis no processo". Além disso, a Lei nº 11.690/2008 introduziu no Código de Processo Penal o tratamento das provas ilegais, por meio do artigo 157, que proíbe sua utilização no processo penal, exigindo que sejam retiradas, ou "desentranhadas", do processo. Portanto, se uma interceptação telefônica é realizada de forma a torná-la ilegal, ela deve ser excluída do processo, pois viola a intimidade, a privacidade ou a dignidade das pessoas envolvidas (Lopes, 2019).

Ainda, há a chance de a prova ser tida como ilícita em razão de ir contra o princípio constitucional, como na hipótese da gravação de conversa telefônica que exponha o interlocutor ao ridículo, afrontando assim, com o resguardo da imagem, a vida privada e a

intimidade (Capez, 2019).

Igualmente, os dados obtidos por meio da interceptação telefônica são restritos à sua motivação de requerimento, sob risco de ocorrer o desvio ilegal. Constitui um exemplo a autorização judicial para uma interceptação telefônica para averiguar o crime de tráfico de substâncias entorpecentes, porém, posteriormente utilizar essas mesmas informações para instaurar processo criminal diverso pelo crime de sonegação fiscal (Lopes, 2019).

Dessa maneira, na hipótese de ilícito desvio causal da prova autorizada para apurar um crime, é considerada uma ilegalidade, não sendo admissível e causando a nulidade desse novo processo que gerou o ilegal desvio causal (Lopes, 2019).

2.8 DO SIGILO DOS DADOS OBTIDOS

No quesito de sigilo de dados telefônicos, este se encontra respaldado pela Lei de InterceptaçãoTelefônica, contudo ainda é utilizada a Lei n° 9.296/96, a fim de determinar os requisitos, a abrangência e os limites, servindo de parâmetro para o Juiz na hora de permitir a quebra do sigilo dos dados telefônicos (Capez, 2016).

É importante frisar o princípio da intranscendência, o qual determina que a pena não pode passar do réu, logo, a acusação apenas pode pesar sobre o autor, coautor ou partícipe do crime (Lopes, 2019).

Nesse sentido, a ação penal e suas provas produzidas englobam apenas a pessoa a que se imputa a prática do delito, sendo vedada sua extensão a terceiros, pois advém do princípio previsto no artigo5º, inciso XLV, da Constituição Federal (Capez, 2016).

No caso das quebras de sigilo das telecomunicações, deve haver a preservação do sigilo das diligências, gravações e transcrições, voltando-se para o resguardo da intimidade de terceiros que porventura sejam atingidos durante a realização da prova (Grinover, 1997).

Ainda, é previsto o incidente de inutilização dos trechos de conversa que não interessam para o motivo que fundamentou a prova, visando à garantia da privacidade de estranhos (Grinover, 1997).

A respeito dessa inutilização, é determinada pelo juiz a transcrição dos trechos indicados pela autoridade policial e pelas partes, que são trechos irrelevantes e impertinentes, não convenientes. (Grinover, 1997).

Desse modo, a Constituição Federal expressa em seu artigo 5º, inciso XLV, que nenhuma pena ultrapassará da pessoa do réu (Brasil, Constituição, 1988). Na hipótese de algum abuso para com a intimidade da pessoa, esta pode requerer uma indenização pelo

dano material ou moral sofrido em decorrência da violação, conforme o artigo 5º, inciso X, da Constituição Federal (Brasil, 1988).

No que tange ao sigilo da fonte, o artigo 190-B, da Lei n° 13.441/17 dispõe sobre as informações obtidas por meio da infiltração virtual que estas devem ser encaminhadas ao juiz responsável pela autorização da medida, que zelará pelo seu sigilo. Com o objetivo de assegurar a eficiência da investigação, o parágrafo único do referido artigo estabelece sigilo nas investigações até concluir todas as diligências, determinando acesso aos autos da infiltração somente ao delegado, ao Ministério Público e ao Juiz (Jorge, 2018).

Dessa forma, a Lei de Organização Criminosa prevê, em seu artigo 14, inciso III, que são direitos do agente infiltrado ter sua qualificação, imagem, voz, nome e demais informações de caráter pessoal preservadas no curso das investigações e do processo criminal. No entanto, se isso se aplica ou não ao agente virtual, faz-se imprescindível observar que há uma divergência doutrinária (Jorge, 2018).

A divergência doutrinária se divide na primeira parcela que acredita haver possibilidade de o agente virtual ser ouvido na qualidade de testemunha anônima, de modo que o advogado de defesa possa participar dessa produção probatória. A segunda parcela da doutrina entende que o advogado do acusado não deva participar da audiência da qual o agente infiltrado é ouvido, tendo como argumento a premissa de que o réu se defende de fatos, e não de pessoas (Jorge, 2018).

Por fim, no artigo 5º, inciso LXXV, da Constituição Federal encontra-se manifesto o direito a ressarcimento pelo erro praticado pelo Poder Judiciário (Brasil, 1988).

Diante do exposto sobre as investigações, procedimentos sigilosos e dando ênfase ao princípio da intranscendência, é notório que por muitas das vezes no curso da investigação, seja por interceptação ou por infiltração, a investigação transcende a pessoa do investigado e inevitavelmente atinge terceiros, com danos reais ou danos potenciais incalculáveis, ficando o terceiro praticamente impossibilitado de se defender, pois os atos dos agentes não são postos à fiscalização.

3 CONSIDERAÇÕES FINAIS

Diante de todo o exposto, fica evidente que, embora o direito digital, de forma geral, tenha progredido muito ao longo dos anos e continue progredindo, faz-se necessário observar as lacunas e falhas que permeiam a sociedade digital das pessoas, principalmente se levarmos em conta que temos mais informações de nossas vidas no mundo digital do que

no mundo real.

Desse modo, torna-se imperativo observar as lacunas e deficiências mencionadas anteriormente, tanto na legislação que objetiva proteger os dados individuais, a qual frequentemente revela falhas e ainda ocasiona vazamentos de informações, na esfera da internet ou da *deep web*, para uma ampla gama de propósitos, bem como na condução de investigações policiais por agentes do Estado, dada a natureza humana dessas atividades. É necessário considerar que tais atividades são conduzidas por seres humanos, os quais estão suscetíveis a preconceitos, opiniões, desejos e, sobretudo, ao conceito de fé pública, que pressupõe a veracidade de suas ações.

Importante se faz ainda ressaltar que, embora a legislação sobre direitos digitais tenha progredido exponencialmente ao longo dos últimos anos, um importante evento que deve ser combatido é a exposição de dados de terceiros não investigados em inquéritos e processos judiciais, pois essa exposição, mesmo que autorizada por um juiz, gera danos reais ou potenciais ao terceiro, uma vez viola sua privacidade e intimidade sem que necessariamente tenha contribuído com algum ilícito penal.

Nesse sentido, o Estado não pode atuar como um leviatã desenfreado para executar seus objetivos. Assim, freios, regras e contramedidas devem surgir, como hipótese, uma espécie de juiz das garantias, seja por meio de um representante do Judiciário ou do Ministério Público para fiscalizar a atuação da inteligência dos órgãos de investigação, de modo que assegure que não haverá mau uso do poder do agente público.

Além disso, considera-se imperiosa a criação de auditorias independentes com a finalidade de fiscalizar os sistemas e processos utilizados pelas agências governamentais responsáveis pelas investigações, objetivando dessa forma identificar violações de privacidade ou quebras de protocolos por parte dos agentes públicos.

Ademais, também é importante a adoção de uma proteção jurídica e de incentivos para os denunciantes que alertam para atividades ilegais por parte do Estado, estimulando a revelação de informações sobre violações de privacidade.

É necessário o desenvolvimento de tecnologias de criptografia mais avançada, que proteja os dados e dificulte a invasão dos dispositivos, bem como a criação de sistemas de alerta precoce, que detectem e notifiquem os indivíduos de que seus dados estão sendo vazados, para que ele possa cobrar indenização do Estado por falha de protocolo.

Junto a isso, ainda é necessária a adoção de punições mais rigorosas para o Estado, em casos de violação de privacidade e de vazamento de dados, incluindo sanções administrativas ao agente público e indenizações aos terceiros afetados.

Considerando ainda que hoje vários procedimentos são interligados, como, por exemplo, o boletim de ocorrência da polícia com o Ministério Público, seria interessante a criação de um departamento responsável por filtrar as informações contidas na escuta, codificando informações sensíveis e pessoais de terceiros não envolvidos, e relatando ainda os números atingidos indiretamente pela investigação.

REFERÊNCIAS

BARROSO, Luiz Roberto Barroso. **Curso de Direito Constitucional Contemporâneo**. 2. ed. São Paulo, Saraiva Educação, 2010.

BRASIL, **Constituição da República Federativa do Brasil**, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 out. 2023.

BRASIL, **Lei de Organização Criminosa,** 2013, Disponível em:// https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 17 mar. 2024.

BRASIL, **Convenção de Budapeste,** 2023. Disponível em: //https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm.Acesso em: 17 mar. 2024.

SYDOW, Spencer Toth, et al, **Crimes Informáticos e Suas Vítimas.** 2. ed. São Paulo, Saraiva,2015.

CAPEZ, Fernando Capez, **Curso de Processo Penal**. 23. ed. São Paulo, Saraiva, 2016.

GRECO FILHO, Vicente. **Interceptação Telefônica**, 3. ed. São Paulo, Saraiva, 2015.

GRINOVER, Ada Pellegrini Grinover, **O Regime brasileiro das interceptações telefônicas**,Revista CEJ, 1997.

LOPES, Aury Lopes Jr**. Direito Processual Penal**. 16. ed. São Paulo, Saraiva Educação, 2019. MORAES, Alexandre de Moraes. **Direito Constitucional**. 33. ed. São Paulo, Atlas, 2016.

PINHEIRO, Patricia Peck. **Direito digital**. 7. ed. São Paulo, Saraiva, 2021. E-book.

MINTO, Andressa Olmedo. **A Prova Digital no Processo Penal.** 1. ed. São Paulo, LiberArs, 2021.

ALVES, Matheus de Araújo. **Crimes Digitais:** análise da criminalidade digital sob a perspectivado Direito Processual Penal e do Instituto da Prova**,** 1. ed. São Paulo, Dialética, 2020.

GARCIA, Lara Rocha, et. al., **Lei Geral de Proteção de Dados (LGPD):** Guia de implantação, 1. ed. São Paulo, Blucher, 2019.

FERNANDES, A. S. Provas no Processo Penal - estudo comparado. São Paulo: Saraiva, 2011. E-book.

JORGE, Higor Vinicius Nogueira. **Investigação Criminal Tecnológica.** Volume 1, ed. BRASPORT, 2018.