INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA
COORDENAÇÃO DE PÓS-GRADUAÇÃO
CURSO DE MESTRADO PROFISSIONAL EM DIREITO

VINÍCIUS SEGATTO JORGE DA CUNHA

AVANÇOS TECNOLÓGICOS NA INVESTIGAÇÃO CRIMINAL E O *STANDARD* PROBATÓRIO PARA O ACESSO AOS DADOS ARMAZENADOS EM NUVEM

BRASÍLIA

2025

VINÍCIUS SEGATTO JORGE DA CUNHA

AVANÇOS TECNOLÓGICOS NA INVESTIGAÇÃO CRIMINAL E O *STANDARD* PROBATÓRIO PARA O ACESSO AOS DADOS ARMAZENADOS EM NUVEM

Dissertação apresentada ao Programa de Pós-Graduação em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, como requisito para obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Rogério Schietti Cruz

BRASÍLIA

2025

VINÍCIUS SEGATTO JORGE DA CUNHA

AVANÇOS TECNOLÓGICOS NA INVESTIGAÇÃO CRIMINAL E O *STANDARD* PROBATÓRIO PARA O ACESSO AOS DADOS ARMAZENADOS EM NUVEM

Dissertação de apresentada ao Programa de Pós-Graduação em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, como requisito para obtenção do título de Mestre em Direito.

BANCA EXAMINADORA

_____

Prof. Dr. Rogério Schietti Cruz
Orientador

_____

Prof. Dr. Ney de Barros Bello Filho
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP

_____

Prof. Dr. Vinicius Gomes de Vasconcellos
Universidade de São Paulo – USP

Código de catalogação na publicação – CIP

C972a Cunha, Vinícius Segatto Jorge da

Avanços tecnológicos na investigação criminal e o standard probatório para o acesso aos dados armazenados em nuvem / Vinícius Segatto Jorge da Cunha. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2025.

117 f. .

Orientador: Prof. Dr. Rogério Schietti Cruz

Dissertação (Mestrado Profissional em Direito) — Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, 2025.

1. Investigação criminal. 2. Internet - legislação - Brasil. 3. Prova criminal - Brasil. 4.Proteção de dados pessoais. I.Título

CDDir 341.434

Elaborada por Natália Bianca Mascarenhas Puricelli – CRB 1/3439

RESUMO:

Esta pesquisa terá como finalidade confrontar a jurisprudência consolidada pelos Tribunais pátrios e pela Suprema Corte sobre a (in)violabilidade dos fluxos de comunicação e dados armazenados por indivíduos investigados. Segundo a jurisprudência, a quebra de sigilo de dados armazenados não está abrangida pela Lei 9.296/96, pois não se trata de interceptação, mas de acesso às informações armazenadas, sendo, na visão dos Tribunais, aplicável a Lei do Marco Civil da Internet. No entanto, a Lei 12.965/2014 não foi criada com o propósito de regulamentar e definir os parâmetros e os procedimentos a serem adotados em investigação criminal e em instrução processual quando necessário o acesso e a obtenção dos dados e informações armazenadas pelo investigado. Afinal, é sabido que o telefone celular e os aparelhos inteligentes carregam consigo todas as informações relativas ao seu proprietário, desde a contabilização de passos e demarcação de percursos em uma caminhada realizada até o numerário bancário. Isso reflete a vastidão dos arquivos contidos nos aparelhos em uso e, consequentemente, dos dados digitais salvos, exigindo atenção ao espectro de proteção constitucional contido no artigo 5º, X, XII e LXXIX, da Constituição da República, diante da ausência de regulamentação legal específica para a efetivação de eventual medida de acesso às informações e dados do acusado armazenados em seus aparelhos e salvos remotamente.

Palavras-chave: *Standard* probatório. Quebra de sigilo. Investigação criminal. Armazenamento em nuvem de dados digitais. Lei do Marco Civil da Internet.

ABSTRACT:

This research aims to confront the consolidated jurisprudence of domestic courts and the Supreme Court regarding the (in)violability of communication flows and data stored by individuals under investigation. According to jurisprudence, the disclosure of stored data is not covered by Law 9.296/96, as it pertains not to interception but to access to stored information, viewed by the courts as governed by the Brazilian Internet Civil Rights Framework Law. However, Law 12.965/2014 was not designed to regulate and define parameters and procedures for accessing stored data in criminal investigations and procedural instructions. It is well known that mobile phones and smart devices carry extensive personal information, from step counts during walks to banking details, highlighting the breadth of data stored on these devices. This necessitates attention to the constitutional protections under Articles 5, X, XII, and LXXIX of the Federal Constitution, given the absence of specific legal regulation for accessing and retrieving accused individuals' remotely stored information and data.

Keywords: Probationary standard. Breach of confidentiality. Criminal investigation. Cloud storage of digital data. Internet Civil Framework Law.

LISTA DE ABREVIATURAS E SIGLAS

AgRg – Agravo Regimental

CPP – Código de Processo Penal

CRFB – Constituição da República Federativa do Brasil

DSEL – Lista de Sujeitos Desacreditados sob Execução

F3EAD – Find, Fix, Finish Exploit Analyze and Disseminate[1]

HC – *Habeas Corpus*

IA – Inteligência Artificial

IP – *Internet Protocol Address*

LGPD – Lei Geral de Proteção de Dados

LOA – Lei de Organização Criminosa

SDC – Sistema de Crédito Social

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

TJDFT – Tribunal de Justiça do Distrito Federal e dos Territórios

[1] Encontrar, Corrigir, Finalizar, Explorar, Analisar e Disseminar. Tradução Livre.

SUMÁRIO

INTRODUÇÃO

A linha histórica da sociedade, sinalizada por relevantes transições como a "Revolução Industrial" entre os anos de 1760 e 1840, possui marcos consagrados de evolução com transformações no modo de produção e nas relações de trabalho. Em meados do século XX, a história foi marcada pela "Era da Informação" com a ascensão da tecnologia caminhando para a atual *era digital* ou *big data*, referente à sociedade da informação ou de dados.

Em decorrência disso, a ciência tecnológica impacta diretamente o meio industrial, empresarial, o comportamento humano e as relações sociais, de modo que hábitos anteriormente tradicionais, a exemplo das ligações por telefone fixo, da máquina fotográfica, do acesso presencial a bancos, mercados, farmácias e cinemas, bem como dos pagamentos em papel-moeda, podem ser efetivados por um único item: o *smartphone*.

Nele, o indivíduo não apenas pratica atos essenciais à sua sobrevivência, mas também deposita integralmente todos os dados e itens que reputar necessários, efetuando quase plenamente os atos da vida cotidiana, de modo que a dependência do *smartphone* e dos mecanismos a ele inerentes não se resume apenas ao vício, mas à sujeição vital diante daquilo que é fornecido e definido apenas por um *click*.

A comunicabilidade cibernética e telefônica atualmente possui uma gama de possibilidades. A integração das redes oferta aos consumidores incontáveis aplicativos como instrumentos de transmissão, recepção de mensagens e contatos instantâneos, a exemplo do *Telegram, WhatsApp*, Mídias Sociais (*Instagram, Facebook, X/Twitter*), *drives,* dentre outros, nos quais armazenam quase todas as informações referentes às suas vidas pessoais.

Nessa perspectiva, como instrumento à persecução penal para colheita de elementos probatórios, tem sido usual a quebra de sigilo desses dados e arquivos através de medidas como a interceptação de dados telemáticos dos aparelhos eletrônicos do indivíduo investigado, além do acesso aos dados armazenados em nuvem ou no disco rígido dos aparelhos, sem o respectivo *backup*, com a consequente descoberta das informações nele constantes.

A título de exemplo, mecanismos como *spywares*, definidos como *softwares* maliciosos projetados para coletar informações dos usuários sem o consentimento do usuário, podem registrar atividades em computadores e dispositivos móveis, alterando páginas da *web* e capturando dados pessoais, senhas e até mesmo imagens em tempo real.

Tais *softwares*, cujos principais provedores são pessoas jurídicas instituídas no exterior, são vendidos na *internet* e podem ser adquiridos por qualquer pessoa que detenha condições financeiras, não sendo o acesso limitado aos órgãos públicos com atribuições investigativas.

Sendo assim, a problemática da vulnerabilidade do acesso aos dados se deve à ausência de *standards* específicos de fundamentações judiciais para autorizar os procedimentos a serem adotados pelo corpo investigativo, especialmente quando as medidas invasivas alcançam informações de cunho personalíssimo, com expressa proteção nos incisos X, XII e LXXIX do artigo 5º da Constituição Federal.

Na prática, a legislação que mais confere proteção ao sigilo dessas fontes em relação às demais normas é a Lei Federal 9.296 de 24 de julho de 1996, que define a interceptação de comunicações telefônicas e institui seus requisitos, pois prescreve um procedimento mínimo a ser observado tanto pela Autoridade Policial quanto pelo Ministério Público e pelo respectivo órgão julgador para o acesso aos dados, além de ser voltada especificamente às provas em investigação criminal e em instrução processual penal.

Sucede-se, entretanto, que, de acordo com a jurisprudência predominante tanto no Superior Tribunal de Justiça quanto no Supremo Tribunal Federal, a quebra de sigilo de dados armazenados não está abrangida pelo padrão de fundamentação judicial estipulado pela Lei que disciplina a inviolabilidade das comunicações telefônicas (Lei Federal 9.296/96), sob o argumento de que não há interceptação, mas acesso às informações armazenadas, como se fossem meros documentos físicos, em analogia ao artigo 232 do Código de Processo Penal.

Por conseguinte, entendem a doutrina e a jurisprudência ser aplicável a tais casos tão somente a Lei Federal 12.965/2014 (Lei do Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil, instituindo uma série de diretrizes a serem observadas pelos entes federativos, pelos provedores, pelas empresas e usuários.

Nesse cenário, o Marco Civil da Internet, que não é voltado à investigação criminal e não define diretrizes tão sólidas quanto às da Lei 9.296/96 para o acesso e obtenção dos dados e informações armazenadas na "nuvem" e no disco rígido do aparelho telefônico, e tampouco tece qualquer regulamentação sobre o uso indiscriminado de *spywares* pelos agentes públicos, acaba por ser utilizado como legislação principal para acesso aos dados pessoais sensíveis no decorrer das investigações.

Embora compreendam os Tribunais Pátrios que o acesso em voga se refere apenas a "dados em si mesmo", sendo aplicável a Lei 12.965/2014, este trabalho demonstrará que a interceptação telefônica possui como espectro a "intimidade e privacidade" do indivíduo tão somente durante o diálogo telefônico, em aspecto meramente momentâneo.

Por outro lado, o acesso aos itens armazenados em *smartphones* e respectivas "nuvens" são significativamente mais amplos: não há critério ao que será mínima ou completamente acessado; inexiste parâmetro mínimo à inviolabilidade, bastando ordem judicial com respaldo em "mínimos indícios", em efetivo risco ao decisionismo genérico.

O acesso ao aparelho celular do investigado, então, permite uma extensa e detalhada "descoberta" sobre sua vida privada e íntima, pois a obtenção do acervo probatório não é instantânea e limitada à relação de diálogo estabelecida pelo indivíduo através de uma ligação por telefonia, como é o caso da interceptação telefônica. Os agentes atuantes possuem pleno e amplo acesso a vídeos, fotos, arquivos, histórico de pesquisa, dados pessoais, informações bancárias e fiscais, *e-mails,* senhas salvas*,* aplicativos de cunho íntimo e pessoal, dentre tantos outros elementos que possuam ou não relação com os fatos perquiridos.

Nesse aspecto, o trabalho em apreço busca explorar essas questões, analisando como as inovações tecnológicas - considerando todo seu potencial de exposição da intimidade e da vida privada - impactam o *standard* probatório das decisões judiciais para o acesso aos dados armazenados em nuvem durante as investigações criminais.

Dito isto, o objetivo principal deste trabalho é investigar como os avanços tecnológicos, especialmente no que se refere ao armazenamento de dados em nuvem, influenciam o *standard* probatório do qual se valem as decisões judiciais para deflagração e condução das investigações criminais no Brasil, propondo diretrizes que garantam a proteção dos direitos fundamentais dos indivíduos sob a ótica da Lei 9.296/96 (Lei de Interceptação Telefônica) e Lei 12.965/14 (Marco Civil da Internet).

Ademais, os objetivos secundários deste trabalho buscarão analisar a legislação penal brasileira à luz das transformações digitais e seu impacto nas investigações criminais, examinar os métodos investigativos utilizados pelas autoridades policiais e a eficácia das operações policiais no contexto atual, bem como avaliar a coleta e o uso de informações obtidas de aparelhos telefônicos nas investigações, considerando as implicações legais e éticas, além de discutir a Lei 12.965/2014 e a jurisprudência brasileira sobre o acesso a dados armazenados eletronicamente, identificando lacunas, desafios e propondo soluções.

No decorrer do trabalho, foram ponderados os detalhes inerentes a essa inviolabilidade e os limites a serem exercidos, tendo em vista ao período em apuração, aos elementos específicos a serem angariados e à forma de controle e monitoramento desse acesso.

Assim, foram levantadas as seguintes hipóteses: As decisões judiciais podem fundamentar a interceptação telemática e o acesso aos dados armazenados em nuvem tão somente a partir do Marco Civil da Internet, sem observar o *standard* de fundamentação previsto na Lei de Interceptação Telefônica? Após o acesso aos referidos dados, como se dará a sua gestão pelos órgãos encarregados da persecução criminal?

A metodologia adotada para a realização desta pesquisa será de natureza qualitativa, utilizando uma abordagem analítica e descritiva. A pesquisa será baseada em uma revisão bibliográfica abrangente, incluindo artigos acadêmicos, legislação pertinente, decisões judiciais do Superior Tribunal de Justiça e do Supremo Tribunal Federal, bem como relatórios de órgãos de segurança pública.

Além disso, toda a jurisprudência coletada será retirada diretamente dos *sites* oficiais do Superior Tribunal de Justiça e do Supremo Tribunal Federal, sendo disponibilizado ao leitor, no decorrer de cada citação jurisprudencial, as palavras-chave utilizadas para a pesquisa de cada julgado.

Através desta metodologia, pretende-se apresentar as questões e problemáticas do tema indicado e, ainda, destacar a insuficiência da regulação sobre o acesso aos dados do investigado armazenados em nuvem no decorrer das investigações criminais, bem como a necessidade de se resguardar o campo de proteção esboçado pela Constituição Federal em seu artigo 5º, incisos X, XII e LXXIX.

No primeiro Capítulo, serão abordadas as transformações históricas e tecnológicas mais recentes em conjunto com as mudanças no comportamento humano, industrial e social otimizado pelo universo de informações digitais. Será realizada uma análise crítica da legislação penal brasileira, considerando as mudanças trazidas pela era digital, incluindo a discussão sobre os desafios que a legislação enfrenta para se adaptar às novas realidades tecnológicas, sempre considerando a proteção da privacidade e a eficácia das investigações.

O primeiro subtópico abordará a evolução da sociedade da informação e o papel da inteligência artificial nas investigações criminais. Será discutido se a automação e a análise de dados por meio de algoritmos estão substituindo a análise crítica e a interpretação humana, e quais são as implicações disso para o sistema de justiça.

Ainda, serão explicitados como funcionam e quais são os exemplos mais corriqueiros de armazenamento de dados. Será explicada a finalidade dos algoritmos e informações digitais, bem como suas respectivas funcionalidades, a fim de que seja construído gradualmente um glossário jurídico-digital necessário à ciência daqueles que com eles atuam juridicamente.

Por sua vez, no Segundo Capítulo, o enfoque se dará à persecução penal brasileira propriamente dita, seu contexto histórico e legal, incluindo o direito penal probatório e as ferramentas disponíveis às autoridades investigativas e acusatórias no âmbito da violabilidade de dados e informações coletadas em aparelho telefônico e dados armazenados remotamente. Aqui, será explorada a estrutura da persecução penal no Brasil, destacando os principais atores envolvidos e os procedimentos utilizados. A análise incluirá a relação entre a tecnologia e a eficácia das investigações.

Em seu primeiro subtópico, serão examinados os métodos investigativos utilizados pelas autoridades policiais, com foco nas operações policiais de grande escala. Serão discutidos os critérios que levam à deflagração dessas operações e a eficácia dos métodos empregados.

No segundo subtópico, será analisada a coleta de dados de aparelhos telefônicos, incluindo as técnicas utilizadas e as implicações legais, a exemplo do uso de *spywares* e seu perigo ante à ausência de regulamentação. A discussão incluirá a proteção dos direitos dos indivíduos e a necessidade de um equilíbrio entre segurança e privacidade.

No terceiro subtópico do segundo capítulo, será abordada a Lei 12.965/2014, conhecida como Marco Civil da Internet, e sua aplicação na jurisprudência brasileira. Serão discutidos os desafios enfrentados na interpretação da lei em relação ao acesso a dados armazenados eletronicamente, bem como as decisões judiciais que moldam esse campo.

Com isso, será retratada a metodologia utilizada pelas recentes Operações Policiais deflagradas que utilizam informações obtidas mediante acesso "desburocratizado" aos dados e informações armazenados em nuvem do indivíduo investigado, seja para indício de prova ou para elaboração de Relatórios de Inteligência Financeira, bem como para subsidiar representação por medidas cautelares ao longo da perquirição pré-processual.

No terceiro capítulo, serão discutidos os *standards* probatórios e padrões de fundamentação judicial para garantir a segurança jurídica no acesso, uso e gestão de dados armazenados.

Por fim, a pesquisa será encerrada com uma análise constitucional sobre a temática, com a finalidade de se reequilibrar a aplicação das medidas de acordo com o impacto em que cada uma exerce no âmbito de proteção indicado pelo constituinte através da Constituição da República, apresentando propostas para a elaboração de legislação que confira segurança jurídica no que concerne às decisões judiciais que autorizam a quebra da privacidade dos investigados para o acesso aos seus dados e arquivos armazenados em nuvem.

1. A PROTEÇÃO LEGISLATIVA DE DADOS NA ERA DIGITAL

O Código de Processo Penal e o Código Penal possuem mais de oitenta anos de existência. Ambos os Decretos-Leis foram promulgados durante a "Era Vargas", um período ditatorial conhecido como "Estado Novo", que foi marcado pela censura, centralização do poder e limitação das liberdades civis.

Isso significa, então, que ambos nasceram em uma conjuntura totalitária e obedeceram exclusivamente à vontade do ex-Presidente Getúlio Vargas. Além disso, seus processos de criação não passaram pelo processo legislativo democrático com a aprovação pelo Senado Federal e pela Câmara dos Deputados. Apesar de existirem posições em contrário, parte da doutrina considera o Código de Processo Penal brasileiro como uma "cópia inquisitiva" do Código Rocco italiano de 1930, que estava em vigor durante a ditadura fascista de Mussolini[2].

A retrospectiva do contexto em que as duas principais legislações penais foram criadas é fundamental diante das circunstâncias postas à época e dos instrumentos que influenciaram nas escolhas realizadas pelo Chefe de Estado, não apenas em relação à concentração de poder, mas da essência das normas utilizadas.

Sendo assim, consoante expôs Luiz Edson Fachin sobre Processo Penal, Tecnologia e Democracia, a legislação penal é o resultado da atuação política de uma sociedade, consignando, ainda, que:

> Nessa esteira, partindo-se da premissa de que a legislação penal é o resultado de um ato político de uma sociedade, organização que define o que é crime e de alguma forma, também institui quem é criminoso, no plano do direito processual penal, nos questionamentos acerca de em que medida ele é também resultado de uma decisão política. Se o seu desenvolvimento é atravessado pelas deliberações políticas em sentido amplo, não apenas parlamentares, mas de um debate social engajado na

[2] "It's known that the Rocco Code and Napoleonic Code represented models of modern procedural techniques and one can imagine their influence in the European-continental tradition legislation in the first half of the twentieth century. However, the jurists responsible for produce the Criminal Procedure Code of 1941 always said that the goal was make a legislation that would answer national needs, "tailored for Brazil." - Sabe-se que o Código Rocco e o Código Napoleônico representaram modelos de técnicas processuais modernas, e pode-se imaginar sua influência na legislação da tradição europeia-continental na primeira metade do século XX. No entanto, os juristas responsáveis pela elaboração do Código de Processo Penal de 1941 sempre afirmaram que o objetivo era criar uma legislação que atendesse às necessidades nacionais, 'feita sob medida para o Brasil'" (Tradução livre do inglês). ABREU, F. Princípios informativos do Código de Processo Penal. Revista Forense, Rio de Janeiro, v. XCVI, a. XL, fasc. 424, out. p. 5-11, 1943. In: BORGES, Clara Maria Roman. **A genealogy of the critical discourses on the authoritarianism of the Brazilian Criminal Procedure Code**. Sequência (Florianópolis) [Internet]. 2021;42(87):e63139. Disponível em: https://doi.org/10.5007/2177-7055.2021.e63139. P. 14.

> busca de um processo penal justo, que controle as interferências estatais no patrimônio e nas liberdades do indivíduo, devidamente legitimadas no contexto da proteção dos direitos fundamentais daqueles contra quem a persecução é executada, como dos outros em favor de quem se restaura direitos ou os previne de violação[3].

Conforme o excerto citado, é abordada a ideia de que a legislação penal é essencialmente um produto político que reflete as decisões de uma sociedade sobre o que constitui crime e quem é considerado criminoso. Além disso, questionam os autores até que ponto o direito processual penal também é resultado de decisões políticas, afinal, seu desenvolvimento é influenciado por deliberações políticas amplas, não limitadas ao parlamento, mas incluindo um debate social engajado.

Esse debate, por sua vez, tem como objetivo o alcance de um processo penal justo, que equilibre o controle das intervenções do Estado sobre os bens e liberdades dos indivíduos com a proteção dos direitos fundamentais daqueles contra quem o processo é dirigido, objetivos esses os quais podem ser alcançados pela restauração ou prevenção de violações de direitos individuais ou coletivos.

Nessa perspectiva, para além de as duas principais legislações na seara criminal serem octogenárias e frutos de um governo eminentemente autoritário, não possuem expectativas próximas ou concretas de sofrerem radical mudança em seu texto (a exemplo do Projeto de Lei 8.045 que cria o novo Código de Processo Penal e está pendente de aprovação definitiva desde 2010); e sequer estão em devida harmonia com a Constituição Federal.

Nesse contexto, a Constituição da República garante em seu artigo 5º, X, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Isso significa que ninguém pode ter sua privacidade violada sem consentimento, sendo garantido o direito à indenização por danos morais ou materiais resultantes dessa violação.

Ademais, o artigo 5º, XII, da Constituição estipula o sigilo da correspondência e das comunicações telegráficas, exceto em casos determinados por ordem judicial, para investigação criminal ou instrução processual penal. Essa medida visa garantir a privacidade nas comunicações, permitindo interferência estatal apenas sob rigorosos

[3] FACHIN, Luiz Edson; ESTEVES, Fabio Francisco. **Processo Penal, Tecnologia e Democracia**. Org.: MADEIRA, Guilherme; BADARÓ, Gustavo; SCHIETTI, Rogerio. **Código de Processo Penal: Estudos Comemorativos aos 80 anos de Vigência**: Vol. 1. São Paulo: Thomson Reuters Brasil, 2021. P. 264.

critérios legais e processuais, salvaguardando direitos individuais contra eventuais abusos.

A respeito disso o artigo 9º do Marco Civil da Internet estabelece que os provedores de internet devem tratar todos os dados que trafegam em suas redes de maneira igualitária, sem discriminação baseada no conteúdo, origem, destino ou aplicação dos pacotes de dados, garantindo aos usuários o acesso irrestrito aos conteúdos na internet, sem interferências que possam prejudicar a velocidade ou bloquear o acesso a determinados sites.

Outrossim, inserido recentemente, o inciso LXXIX do artigo 5º da Constituição Federal assegura o direito à proteção dos dados pessoais nos meios digitais, conforme previsão legal, tratando-se de norma constitucional de eficácia limitada. Essa proteção visa garantir que informações pessoais sejam tratadas de forma segura, impedindo seu uso indevido ou sem consentimento.

A respeito da inserção do novo inciso ao artigo 5º da Constituição da República, ressaltando a proteção constitucional aos dados armazenados, confira-se as seguintes considerações da doutrina de Ingo Sarlet:

> Com a aprovação da PEC 17/2020 e posterior promulgação (fevereiro de 2022) da correspondente EC 115/22, a discussão sobre a conveniência e oportunidade da inserção de um direito à proteção de dados pessoais na CF, ficou, de certo modo, superada. De acordo com o texto da EC 115, foi acrescido um inciso LXXIX ao artigo 5º, CF, dispondo que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". (Incluído pela Emenda Constitucional nº 115, de 2022).
> Mesmo que se pudesse, como já o fizera o STF, reconhecer a proteção de dados como um direito fundamental implícito, daí extraindo todas as consequências atinentes à tal condição, o fato é que sua positivação formal, em sendo o caso, carrega consigo uma carga positiva adicional, ou seja, agrega (ou, ao menos, assim o deveria) valor positivo substancial em relação ao atual estado da arte no Brasil.[4]

Foi contemplado, assim, o direito à privacidade no intuito de proteger os dados pessoais dos usuários, exigindo consentimento expresso para qualquer operação com essas informações. Além disso, determina que violações à intimidade, comunicações

[4] SARLET, Ingo. **A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I**. Consultor Jurídico. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental/. Acesso em 11.03.2024.

sigilosas e à vida privada devem ser indenizadas tanto moral quanto materialmente, assegurando a segurança e o respeito à privacidade dos cidadãos na era digital.

Desse modo, a formalização deste direito como fundamental traz, nos dizeres de Ingo Sarlet, "uma carga positiva adicional", que vai além do reconhecimento implícito anteriormente feito pelo Supremo Tribunal Federal, pois a positivação cria um marco jurídico claro e robusto, fornecendo uma base sólida para a criação de leis específicas que regulamentem o uso, armazenamento e compartilhamento de dados pessoais, especialmente no contexto digital, o que também é essencial em um cenário onde a tecnologia e a inteligência artificial estão cada vez mais integradas ao cotidiano das pessoas e às operações das instituições.

Nesse contexto, em resposta aos avanços tecnológicos que impactam diretamente as relações interpessoais e jurídicas, surgiu na doutrina o termo denominado "constitucionalismo digital"[5]. Dentre seus principais desafios, é destacada a proteção dos direitos individuais em face das ações de empresas privadas, como as plataformas digitais, que têm um papel cada vez mais importante em funções públicas, como a moderação de conteúdo e o banimento de usuários:

> Um dos grandes desafios do constitucionalismo digital - talvez o maior de todos - consiste na proteção de direitos de indivíduos contra ações de atores privados que desempenham funções públicas ou "quase públicas". É o caso das plataformas digitais, que se tornaram a nova arena do debate público e têm levantado preocupações na tomada de decisões voltadas à moderação de conteúdo e banimento de usuários. Não por acaso, a origem do constitucionalismo digital teve como foco inicial a preocupação com a limitação do exercício de poder por agentes privados na internet, em oposição à limitação do poder estatal.[6]

Ainda, convém enfatizar o fenômeno da mutação constitucional, que é o processo pelo qual o significado de uma norma prevista na Constituição pode ser alterado sem a necessidade de se modificar formalmente seu texto. Nesta hipótese, ao invés de ser formulada uma emenda ou revisão constitucional, a mudança ocorre a partir da atribuição de sentido diverso à norma, tendo como base os valores atualizados da sociedade acerca do comando constitucional em mutação.

---

[5] "A resposta a esse conjunto de preocupações é denominada constitucionalismo digital, que tem sido particularmente fortalecido no continente europeu. Tal fenômeno pode ser compreendido como um conjunto de iniciativas jurídicas que objetivam articular o exercício de direitos políticos, normas de governança e limitações ao exercício do poder no ambiente digital.". LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. 2.ed., rev. e atual. 2 São Paulo: Editora JusPodivm. 2024. P. 158-159.

[6] Ibidem. p. 159.

Assim explica o fenômeno a lição doutrinária de Gilmar Ferreira Mendes e Paulo Gustavo Gonet Branco:

> O estudo do poder constituinte de reforma instrui sobre o modo como o Texto Constitucional pode ser formalmente alterado. Ocorre que, por vezes, em virtude de uma evolução na situação de fato sobre a qual incide a norma, ou ainda por força de uma nova visão jurídica que passa a predominar na sociedade, a Constituição muda, sem que as suas palavras hajam sofrido modificação alguma. O texto é o mesmo, mas o sentido que lhe é atribuído é outro. Como a norma não se confunde com o texto, repara-se, aí, uma mudança da norma, mantido o texto. Quando isso ocorre no âmbito constitucional, fala-se em mutação constitucional. A nova interpretação há, porém, de encontrar apoio no teor das palavras empregadas pelo constituinte e não deve violentar os princípios estruturantes da Lei Maior; do contrário, haverá apenas uma interpretação inconstitucional.[7]

Como visto, tal fenômeno é resultado da atividade do poder constituinte difuso[8], o qual se refere à capacidade dos diversos agentes do sistema político e jurídico de reinterpretar as normas constitucionais. A mutação constitucional permite que a constituição se adapte às novas realidades sociais, políticas e econômicas sem a necessidade de um processo formal de alteração do texto normativo.

A mutação constitucional pode ocorrer de diferentes formas, incluindo a interpretação judicial, onde os tribunais reavaliam e reinterpretam as normas à luz das circunstâncias atuais, e as práticas legislativas e administrativas que introduzem novos entendimentos das normas constitucionais. Esse processo é essencial para a flexibilidade e a evolução do direito constitucional, garantindo que a constituição permaneça relevante e eficaz ao longo do tempo.

A importância da mutação constitucional reside na sua capacidade de manter a constituição viva e dinâmica, permitindo que ela se adapte sem a necessidade de procedimentos formais, e muitas vezes complexos, de emenda. Esse mecanismo ajuda a

---

[7] MENDES, Gilmar F.; BRANCO, Paulo G. G. **Curso de Direito Constitucional**. Saraiva, 2013. E-book. P. 201.

[8] "Diferentemente do poder constituinte derivado – que é um poder de direito, estatuído e previamente regulamentado –, o poder constituinte difuso define-se como um poder de fato, pois não é estatuído e surge a partir de uma necessidade social, sendo espontâneo e exercido apenas quando há necessidade. O poder constituinte difuso é responsável pela modificação da constituição e atua através das mutações constitucionais que têm por finalidade alterar apenas o sentido e alcance das normas constitucionais, deixando o texto constitucional intacto e evitando, assim, uma instabilidade textual da carta magna.". ARNAUD, Raraela Rocha; TARGINO, Giliard Cruz; ESTRELA, William Marques. **Mutação constitucional: A atuação do poder constituinte difuso no Brasil**. Revista Interdisciplinar e do Meio Ambiente-ISSN 2674-693X -v.1, n.1, 2019, e41. P. 4. Disponível em: https://caroa.org.br/revista/index.php/rima/article/view/59/21 Acesso em 11.02.2024.

equilibrar a estabilidade do texto constitucional com a necessidade de evolução e adaptação contínua, respondendo às demandas de uma sociedade em constante mudança.

Ainda assim, muito embora a Carta ulterior não tenha revogado as leis penais por completo, é cediço que as essências de cada não confluem entre si, e, para que seja respeitada a vontade do Constituinte Originário, ao longo desses anos leis penais foram criadas a fim de acompanhar (ou ao menos tentar) as mudanças constantes.

No âmbito infraconstitucional, tem-se como exemplo a promulgação do "Pacote Anticrime", Lei Federal 13.964/19, que trouxe diversos pontos no intento de, conforme sua autodescrição, "aperfeiçoar a legislação penal e processual penal". Com isso, houve substancial alteração de vários dispositivos do Código Penal, do Código de Processo Penal, da Lei de Execução Penal, da Lei dos Crimes Hediondos, entre outras legislações esparsas, a pretexto do "combate à corrupção" no País, no intento de endurecer as penas previstas e sua aplicação.

Apesar de o discurso para a promulgação do Pacote Anticrime, em primeiro plano, ter ostentado caráter punitivista, diversos pontos positivos contribuíram para o sistema processual penal. Nesse sentido explicam Afrânio Silva Jardim e Pierre Souto Maior Coutinho Amorim:

> De modo geral, as alterações processuais, trazidas pela Lei n. 13.964/19, foram surpreendentemente positivas. A surpresa se dá pelo discurso simplista e punitivista que graça no meio político-jurídico atual, de forma que a aprovação de tal lei nos dá certo alento de que nem tudo está perdido em nosso sistema jurídico.
> Muitos pontos podem e devem ser criticados na citada Lei, especialmente quando examinamos seus aspectos penais e de execução penal.
> Mesmo na seara processual, antes da execução penal, há pontos passíveis de críticas, tais como a nova regra do § 5º do art. 157 do CPP, que pode ensejar o uso de provas inadmissíveis apenas com o intuito de afastar o juiz, que assim as declarar, do processo. Melhor solução deu a Lei anterior, de n, 11.690/08, que se limitou a determinar o desentranhamento da prova declarada inadmissível.
> Outro ponto que merece crítica, e que é de duvidosa constitucionalidade, é a regra posta no art. 492, inc. I, alínea "e", do CPP, que agora permite uma execução provisória da pena de prisão, com base no fato da pena ter sido aplicada em patamar igual ou superior a 15 anos. Ora, a questão que se coloca, em relação à (in)constitucionalidade da chamada execução provisória da pena de prisão, é a violação ou não ao princípio da não culpabilidade, pouco importando se a condenação aplicou pena de 10, 15 ou 30 anos.[9]

[9] JARDIM, Afrânio Silva; AMORIM, Pierre Souto Maior Coutinho. **Primeiras Impressões Sobre a Lei n. 13.964/19, Aspectos Processuais**. Org.: MADEIRA, Guilherme; BADARÓ, Gustavo; SCHIETTI, Rogerio. **Código de Processo Penal: Estudos Comemorativos aos 80 anos de Vigência**: Vol. 1. São Paulo: Thomson Reuters Brasil, 2021. P. 388 e 389.

Como exposto, a Lei 13.964/2019 é fruto político e social de demandas à época vindicadas por parcela da sociedade, e, muito embora seja passível de críticas e ponderações, foi elaborada no intento de se moldar as circunstâncias postas naquele período. Diferentemente ocorre, todavia, no campo específico do direito criminal com as diversificadas e intensas mudanças propostas pela "era digital", a qual é contextualizada pela revolução tecnológica, com a difusão massificada de aparelhos telefônicos e eletrônicos afins.

De um planeta analógico, em um curto espaço de tempo o mundo se tornou completamente digital: imóveis automatizados são hoje *smart home*; o relógio tradicional foi substituído por um *smart watch*; os livros físicos por *e-readers;* o telefone fixo pelo *smartphone;* a vassoura comum pelo aspirador robô; o disquete por *pendrive*, o qual mais rápido ainda foi substituído pelo armazenamento em nuvem, que será objeto de especial deliberação nesta pesquisa.

Todos eles possuem uma infinidade de elementos e detêm em comum não só os laços de modernidade e tecnologia, mas a conectividade através da *internet* e do uso da inteligência artificial, com profundo e considerável compartilhamento instantâneo de dados entre dispositivos, os quais usualmente têm sido coletados nos autos de investigações e instruções processuais penais, sendo utilizados como acervo probatório para culpabilizar indivíduos submetidos ao poder punitivo estatal.

Do mesmo modo das mudanças supramencionadas, diligências e medidas investigativas como a interceptação telefônica e a quebra do sigilo telefônico cederam amplo espaço – para não dizer absoluto – à violabilidade dos dados telemáticos e digitais armazenados em dispositivos eletrônicos, sem que a legislação penal e respectivo aparato estejam atentos às transformações e impactos da era digital em seu contexto.

Nesse aspecto, serão analisados neste capítulo os riscos e benefícios dos avanços tecnológicos ocorridos nas últimas décadas, tendo como finalidade contextualizar as críticas, nos próximos capítulos, à orientação jurisprudencial vigente e à adoção de *standards* probatórios para a quebra do sigilo de dados armazenados em nuvem.

1.1. A sociedade da informação e as transformações digitais: a voz pensante foi substituída pela inteligência artificial?

Há longas décadas, a sociedade se encontra em debate sobre o surgimento e o uso de máquinas movidas pela inteligência artificial ao convívio humano, recorrentemente sendo dramatizada através de livros[10] e produções *hollywoodianas* como *Matrix*[11], Resistência[12], O Exterminador do Futuro[13], Inteligência Artificial[14], dentre tantas outras célebres criações.

As obras retratam contextos sob diferentes perspectivas e narrativas, por vezes simbolizando a harmonia entre o homem e o androide[15], apresentando os propósitos e as convencionalidades para as quais foram criadas. Inclusive, os livros e filmes evidenciam as problemáticas do protagonismo robótico em face da submissão humana, e respectiva dependência aos mecanismos tecnológicos pelo próprio homem criados.

Embora a ficção tenha a liberdade e licença poética para teatralizar e tornar mais comoventes os cenários, possui como inspiração aquilo que o mundo real de fato vivencia sob a famosa ideia de que a arte imita a vida e vice-versa. Com isso, a vida do *Homo sapiens sapiens* em sua prática está de fato em constante e completa integração à vida *smart*.

Sob esse enfoque, cabe mencionar que nos anos 2000 fora elaborado por um grupo de cientistas e engenheiros de computação um projeto denominado "*Aware Home*" sob a

[10] *v.g.*, "Eu, Robô", "Androides sonham com ovelhas elétricas?" e "*Neuromancer*"
[11] Estrelado por Keanu Reeves, o filme conta a história de Neo, um programador atormentado por estranhos sonhos, que passa a duvidar do mundo à sua volta. Ao conhecer Morpheus e Trinity, ele descobre estar na Matrix, um sistema de IA que criou uma realidade ilusória e explora seu corpo e cérebro reais. Trazido de volta à consciência, Neo entra então em guerra contra as máquinas, sendo apontado como o messias que pode salvar a humanidade. Disponível em: https://canaltech.com.br/cinema/filmes-imperdiveis-sobre-inteligencia-artificial-49625/
[12] O filme parte do ponto de vista onde a revolução das máquinas acontece de forma precoce, bem como a evolução da inteligência artificial (IA). Disponível em: https://www.techtudo.com.br/guia/2024/01/resistencia-veja-sinopse-elenco-e-critica-do-filme-de-ficcao-cientifica-streaming.ghtml
[13] Um marco entre os filmes sobre Inteligência Artificial. Neste filme de ação, um ciborgue assassino é enviado do futuro para assassinar a mãe do líder da resistência humana. A história aborda a guerra entre humanos e máquinas em um futuro pós-apocalíptico. Disponível em: https://nerdizmo.ig.com.br/21-filmes-sobre-inteligencia-artificial/
[14] [...] ambientado em um futuro onde robôs são usados como companheiros para humanos, o filme segue a jornada de um robô infantil com IA avançada em busca de se tornar humano. Disponível em: https://nerdizmo.ig.com.br/21-filmes-sobre-inteligencia-artificial/
[15] Aparelho ou máquina que se assemelha à figura e aparência humana.

perspectiva de um lar consciente, e dele decorreram outros protótipos para se chegar à hipótese do que se tem hoje como a casa inteligente - ou *smart home*[16].

Ademais, de acordo com a pesquisadora Shoshana Zuboff, a *smart home* – através das plataformas e dispositivos instalados, como é o caso do termostato Nest[17], utiliza sensores de movimento e computação para entender sobre os comportamentos dos moradores de uma casa. Explana, ainda, que:

> Os aplicativos do Nest são capazes de coletar dados de outros produtos conectados, tais como carros, fogões, equipamentos de ginásticas e camas. Tais sistemas podem, por exemplo, disparar luzes quando é detectado um movimento anômalo, acionar gravações de vídeo e áudio e até enviar notificações para os proprietários ou para *outrem.*[18]

Os dispositivos inteligentes – ou *smart devices* – intermediam atos básicos do cotidiano e através da conexão por *Bluetooth*, *Wi-Fi* e inteligência artificial oferecem as mais diversificadas funções aos usuários, desde o preparo de um café à limpeza programada de uma moradia. Para que uma tarefa seja executada, basta a sincronização com um aparelho inteligente e a obtenção de um aplicativo.

Os comandos entre os equipamentos permitem, então, funcionalidades dos eletrodomésticos como ar-condicionado, micro-ondas, máquinas de lavar, fechaduras eletrônicas, entre outros. A conectividade propiciada pela intercomunicação e troca de dados cria, assim, uma verdadeira estrutura tecnológica a favor (ou não) do indivíduo.

Consoante expôs Fábio Luiz Barboza Pereira, a sociedade se encontra cada vez mais dependente da evolução tecnológica e dos benefícios proporcionados, em especial no contexto da Sociedade 5.0, que justifica o uso da tecnologia em prol do desenvolvimento social e econômico. Argumenta, ainda que:

> A 5ª Revolução Industrial, ou Sociedade 5.0, visa à conexão entre sociedade e tecnologia, mediante a convergência entre todas as tecnologias – i.e, inteligência artificial, inteligência das coisas e *cloud computing* – com o objetivo de racionalizar e melhorar a vida das

[16] O mercado global das casas inteligentes era avaliado em 36 bilhões de dólares em 2018 e com estimativa de 151 bilhões de dólares em 2023. ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância. A luta por um futuro humano na nova fronteira do poder**. Tradução de George Schlesinger. 1. ed. - Rio de Janeiro: Intrínseca, 2020. P. 20.

[17] Fabricado por uma empresa que era propriedade da *Alphabet*, a holding dona do Google, que então foi fundida com o Google em 2018. Ele coleta dados sobre seus usos e o ambiente. Ibidem, p. 20.

[18] Ibidem, p. 17.

> pessoas, principalmente nas áreas de infraestrutura, mobilidade urbana e saúde [...][19].

A interdependência do homem com os meios tecnológicos é tamanha que, de acordo com o módulo Tecnologia da Informação e Comunicação da Pesquisa Nacional por Amostra de Domicílios Contínua (Pnad Contínua), divulgada pelo Instituto Brasileiro de Geografia e Estatística (IBGE)[20], 87,2% da população brasileira acima de 10 anos de idade utilizou *internet* no Brasil em 2022, índice que apresentou padrão de crescimento quando comparado aos anos anteriores.

Ainda, a pesquisa divulgada em 2021 em parceria com o Ministério da Ciência, Tecnologia e Inovação apresenta que 90% (noventa por cento) dos lares brasileiros contam com acesso à internet, subsumindo-se a aproximadamente 65,6 milhões de domicílios conectados[21].

Considerando que há no País cerca de 464 milhões de dispositivos digitais funcionais, só entre computador, *notebook*, *tablet* e *smartphone*[22], e deste último há 1,2 por habitante, totalizando a quantia aproximada de 249 milhões de celulares inteligentes em uso, conforme a FGVcia, é possível assim expor que o País vivencia hoje uma integração tecnológica, de modo que raros são os atos cotidianos inexequíveis pelas máquinas e plataformas.

Nessa perspectiva, o conjunto de tecnologias disponíveis e correlacionados coletam e mantém informações do seu possuidor integralmente, e o uso desses dados pelos diversificados ramos coletivos, sociais e institucionais possuem uma infinidade de elementos e detêm em comum não só os laços de modernidade e tecnologia, mas a conectividade através da *internet* e o uso da inteligência artificial, com profundo e considerável compartilhamento instantâneo de dados entre dispositivos.

---

[19] PEREIRA, Fábio Luiz Barboza. **Preocupações sobre a proteção de dados pessoais em veículos autônomos**. Coordenação: PALHARES, Felipe. Estudos sobre Privacidade e Proteção de Dados. São Paulo: Thomson Reuters Brasil. 2021. P. 40.

[20] BELANDI, Caio. **161,6 milhões de pessoas com 10 anos ou mais de idade utilizaram a Internet no país, em 2022**. Agência IBGE Notícias. 09.11.2023. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38307-161-6-milhoes-de-pessoas-com-10-anos-ou-mais-de-idade-utilizaram-a-internet-no-pais-em-2022#:~:text=Destaques,62%2C1%25%20em%202022. Acesso em 10.05.2024.

[21] **90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa**. gov.br. 19.09.2022. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa. Acesso em 10.05.2024.

[22] **Uso de TI no Brasil: País tem mais de dois dispositivos digitais por habitante, revela pesquisa**. Portal FGV. 03.05.2023. Disponível em: https://portal.fgv.br/noticias/uso-ti-brasil-pais-tem-mais-dois-dispositivos-digitais-habitante-revela-pesquisa. Acesso em 10.05.2024.

Com isso, considerando a notória dependência tecnológica que conduziu e vem contribuindo para os avanços da humanidade nas últimas décadas, surgiu a terminologia da "sociedade da informação", a qual pode ser assim explicada:

> Ainda, na conjuntura de atividade social, a informação é considerada um fenômeno entendido no âmbito do conflito estrutural entre os dominantes e os dominados e que a realidade experimentada por cada um, as habilidades desenvolvidas, os objetivos, os conhecimentos adquiridos e as experiências vivenciadas, formam a base de sustentação que possibilita ou impede quaisquer possibilidades. Estas argumentações estão intimamente relacionadas à influência e ao papel que a Ciência e a tecnologia têm desempenhado na sociedade contemporânea, sociedade esta que tem sido identificada na literatura como 'Sociedade da Informação'.[23]

O trecho destaca que, na sociedade contemporânea, a informação desempenha um papel crucial e está envolvida em conflitos estruturais entre grupos dominantes e dominados. A maneira como as pessoas experimentam a realidade, desenvolvem habilidades, estabelecem objetivos, adquirem conhecimentos e vivem suas experiências forma a base que pode facilitar ou impedir suas possibilidades.

Essa dinâmica é influenciada significativamente pela ciência e pela tecnologia, que moldam a "Sociedade da Informação". Neste contexto, a distribuição e o acesso à informação são elementos centrais que podem perpetuar desigualdades ou proporcionar oportunidades.

A propósito, é importante destacar que a inteligência artificial foi elaborada com o objetivo de processar dados de modo mais célere do que um humano ou um *software* comum fariam, pois a IA se utiliza de um processo de automação (*machine learning*) no qual o objetivo é atingido através do raciocínio não biológico, a exemplo do algoritmo.

Além disso, a inteligência artificial utiliza o método do *deep learning*, que é um subcampo do *machine learning* que ensina computadores a processar dados usando redes neurais artificiais, que são inspiradas na estrutura e funcionamento do cérebro humano. Essas redes são compostas por múltiplas camadas de neurônios artificiais que aprendem a identificar padrões em grandes volumes de dados de forma autônoma[24].

---

[23] MARCHI, Késsia Rita da Costa; VALENTIM, Marta Lígia Pomim; BOTEGA, Leonardo Castro. **A Filosofia da informação e a Sociedade da informação e do conhecimento: reflexões diante do progresso tecnológico**. InCID: Revista de Ciência da Informação e Documentação, Ribeirão Preto, Brasil, v. 12, n. 2, p. 32–51, 2021. DOI: 10.11606/issn.2178-2075.v12i2p32-51. Disponível em: https://www.revistas.usp.br/incid/article/view/183305. Acesso em 04.06.2024.

[24] "Por fim, existe a possibilidade de a inteligência artificial tentar imitar a forma de pensamento humano. Nessa situação, os algoritmos tentam replicar a estrutura e a função do cérebro humano (*deep learning*),

Diferente do *machine learning* tradicional, que muitas vezes requer a intervenção humana para identificar características relevantes dos dados, o *deep learning* pode aprender essas características diretamente a partir dos dados brutos, o que o torna particularmente eficaz para tarefas complexas como reconhecimento de imagem, processamento de linguagem natural e detecção de fraudes.

Um recente exemplo do uso de *deep learning* ocorreu em 2016 com a criação da inteligência artificial de jogos de tabuleiro chamada *AlphaZero* pela *Google DeepMind*, responsável por apresentar resultados positivos contra *softwares* já consolidados que não utilizavam a tecnologia do *deep learning*. Conforme informações publicadas em site oficial:

> In chess, AlphaZero first outperformed Stockfish after just 4 hours; in shogi, AlphaZero first outperformed Elmo after 2 hours; and in Go, AlphaZero first outperformed the version of AlphaGo that beat the legendary player Lee Sedol in 2016 after 30 hours. Note: each training step represents 4,096 board positions.
> To learn each game, an untrained neural network plays millions of games against itself via a process of trial and error called reinforcement learning. At first, it plays completely randomly, but over time the system learns from wins, losses, and draws to adjust the parameters of the neural network, making it more likely to choose advantageous moves in the future. The amount of training the network needs depends on the style and complexity of the game, taking approximately 9 hours for chess, 12 hours for shogi, and 13 days for Go.[25]

Assim, o raciocínio lógico de uma Inteligência Artificial (IA) é baseado em algoritmos e modelos matemáticos complexos que permitem à máquina processar informações, identificar padrões e tomar decisões.

Primeiramente, a IA recebe dados de entrada, que podem ser estruturados ou não. Em seguida, esses dados são processados por meio de algoritmos de aprendizado de máquina, redes neurais ou outras técnicas de inteligência artificial. Durante o

---

chamados de redes neurais". NYBO, Erik Fontenele. **Eu, Robô: como dados pessoais podem ser utilizados pela inteligência artificial e os impactos que esse uso pode gerar**. Coordenação: PALHARES, Felipe. Estudos sobre Privacidade e Proteção de Dados. São Paulo: Thomson Reuters Brasil. 2021. P. 89.

[25] "Para aprender cada jogo, uma rede neural não treinada joga milhões de partidas contra si mesma através de um processo de tentativa e erro chamado *reinforcement learning*. No início, ela joga completamente aleatoriamente, mas com o tempo o sistema aprende com vitórias, derrotas e empates para ajustar os parâmetros da rede neural, tornando mais provável a escolha de movimentos vantajosos no futuro. A quantidade de treinamento que a rede precisa depende do estilo e da complexidade do jogo, levando aproximadamente 9 horas para xadrez, 12 horas para shogi e 13 dias para Go." (Livre tradução do autor). SILVER, David. *et al*. **AlphaZero: Shedding new light on chess, shogi, and Go**. Disponível em: https://deepmind.google/discover/blog/alphazero-shedding-new-light-on-chess-shogi-and-go/

processamento, a IA identifica padrões e relações nos dados, utilizando inferência lógica e estatística para extrair informações relevantes.

Com base nesse processo, a IA é capaz de realizar previsões, classificações, otimizações e outras tarefas, adaptando-se e aprendendo com novos dados. Por fim, a IA gera resultados ou respostas com base em seu raciocínio lógico, contribuindo para a automação de processos, tomada de decisões e resolução de problemas em diversas áreas. Nesse aspecto, consoante explica Erik Fontenele Nybo:

> [...] uma inteligência artificial age em cima de dados: seja utilizando dados que a alimentam (inteligência artificial assistida, aumentada ou *machine learning*) seja os dados que ela resolve processar ou usar (inteligência artificial autônoma ou *deep learning*). [...] a base de dados parte de um processo de coleta e organização de dados, realizado por um humano ou por máquinas. [...] Existem diversos mecanismos de coleta, um deles sendo feito por ferramentas de inteligência artificial. [...] Assim, além de apenas processar dados como insumo, a inteligência artificial também pode ter como objetivo encontrar determinados dados e auxiliar na coleta de dados para criação de uma base de dados.[26]

O texto citado explica que a inteligência artificial (IA) trabalha com dados de duas maneiras principais: utilizando dados que a alimentam (como na inteligência artificial assistida, aumentada ou *machine learning*) e processando ou usando dados (como na inteligência artificial autônoma ou *deep learning*). Assim, a base de dados utilizada pela IA é construída a partir de um processo de coleta e organização de dados, que pode ser realizado tanto por humanos quanto por máquinas.

Além disso, a IA não apenas processa esses dados, mas também pode ajudar a encontrar e coletar dados para criar uma base de dados. Isso significa que a IA pode ser uma ferramenta tanto para usar dados existentes quanto para gerar novos dados. Isso, pois há a possibilidade de enriquecimento dessas bases de dados que, sucintamente, consiste em buscar informações extras disponíveis na *internet* e atribuir essas informações a um componente dentro de uma base de dados, tornando-a mais "completa e valiosa".

O desenvolvimento dessas bases de dados seria capaz de perfilar cada pessoa de forma precisa e em escala, definindo grupos através de critérios como os interesses em comum, compras, características compartilhadas, entre outros. Esse levantamento é usualmente utilizado pelos algoritmos do *Google* e do *Facebook* para análise dos seus usuários, com o fito de atingirem suas perspectivas comerciais.

[26] NYBO, op. cit. p. 93.

Ainda, afirma o autor que o complexo de informações está sendo utilizado pelo Estado para realizar políticas públicas, como ocorreu na China através de um sistema de crédito social, ocasião na qual um algoritmo atribuiu nota aos cidadãos conforme suas condutas, definindo se deveriam ou não ter certos direitos e liberdades, baseado em seu comportamento:

> For example, Chinese supreme court invented the 'Discredited Subject under Enforcement List (DSEL)', which backlists those people who refused to obey the court's decision. The second is municipal SCS developed by municipal governments, producing credit scores for local residents with diverse data sources. Scholars have used government documents and media reports to investigate the structure and implementation of the state-centered SCSs. Studies have found that building on multiple governmental agencies' collaborations, SCSs have greatly expanded the scope of surveillance compared with traditional credit systems. For example, mistreating one's parents and running a red light are included in many municipal SCSs' metrics (Liu, 2019). Furthermore, many new punishments have been invented or extended by state-centered SCSs to increase deterrence. For example, people who are put into the DSEL will be punished by having their personal information displayed in public or their travel restricted, along with others. These expanding surveillance and punishment raised serious concerns and heated debates on the state-centered SCSs' relations to the law, privacy, and social norms.[27]

Como visto, o autor discute o sistema de crédito social (SCS) na China, destacando duas formas principais: a "Lista de Sujeitos Desacreditados sob Execução" (DSEL) criada pelo Supremo Tribunal Chinês, que inclui pessoas que não cumpriram decisões judiciais, e os SCS municipais desenvolvidos por governos locais, que geram pontuações de crédito para os residentes usando diversas fontes de dados.

---

[27] "Por exemplo, a Suprema Corte da China inventou a 'Lista de Sujeitos Desacreditados sob Execução (DSEL)', que coloca na lista negra aquelas pessoas que se recusaram a obedecer à decisão do tribunal. O segundo é o SCS municipal desenvolvido pelos governos municipais, produzindo pontuações de crédito para os residentes locais com diversas fontes de dados. Acadêmicos têm usado documentos governamentais e reportagens da mídia para investigar a estrutura e a implementação dos SCSs centrados no estado. Estudos descobriram que, com a colaboração de múltiplas agências governamentais, os SCSs expandiram enormemente o escopo da vigilância em comparação com os sistemas de crédito tradicionais. Por exemplo, maltratar os pais e passar no sinal vermelho estão incluídos nas métricas de muitos SCSs municipais (Liu, 2019). Além disso, muitas novas punições foram inventadas ou ampliadas pelos SCSs centrados no estado para aumentar a dissuasão. Por exemplo, as pessoas que são colocadas na DSEL serão punidas com a exibição de suas informações pessoais em público ou com restrições de viagem, entre outras. Essa expansão da vigilância e das punições levantou sérias preocupações e debates acalorados sobre as relações dos SCSs centrados no estado com a lei, a privacidade e as normas sociais." (Livre tradução do autor). LIU, Chuncheng. **Who supports expanding surveillance? Exploring public opinion of Chinese social credit systems**. International Sociology, 37(3), 391-412. Disponível em: https://doi.org/10.1177/02685809221084446. Acesso em 11.07.2024.

No referido artigo, foi mostrado que esses sistemas, construídos com a colaboração de várias agências governamentais, ampliaram significativamente a vigilância em comparação com os sistemas de crédito tradicionais, de modo que critérios como, por exemplo, maltratar os pais e avançar sinais de trânsito são usados em muitos SCS municipais.

Além disso, novas punições foram criadas ou ampliadas, podendo ser mencionada até mesmo a exibição pública de informações pessoais e restrições de viagem para aqueles que tiveram o nome inserido na DSEL. Esse aumento na vigilância e nas punições levanta sérias preocupações e debates sobre a relação desses SCS com a lei, a privacidade e as normas sociais.

Tem sido comum, então, uma verdadeira customização digital dos usuários, todos elencados pela inteligência artificial através do tratamento da base de dados disponível, em que decisões automatizadas baseadas em dados pessoais afetam o cotidiano, o que pode se dar através dos resultados de buscas; das notícias a serem acessadas; do conteúdo dos contatos em redes sociais[28], entre outros.

Apesar disso, assim como acontece com toda transformação que possua grau elevado de intensidade e abrangência à coletividade, o uso das tecnologias disponíveis e subsidiadas pela inteligência artificial deve ser ponderado com a devida cautela, especialmente quando em uso pelo Estado, tendo em vista a sensibilidade dos dados disponíveis e angariados para consecução das plataformas digitais.

Conforme a visão mais crítica, há uma verdadeira "ditadura" dos algoritmos, pois as escolhas vistas, expressadas ou adquiridas não são mais baseadas na vontade do próprio indivíduo, mas naquilo que os códigos indiretamente influenciam e ordenam, como se quem tomasse a decisão fosse sucedido por procedimentos automatizados com poder demasiado[29].

Acerca da terminologia da "ditadura" dos algoritmos, confira-se lição publicada por Júlia Iunes Monteiro e Marco Aurélio Marrafon:

> Nota-se que, independentemente de sua aplicação por entes públicos ou privados, é frequentemente criticada a legitimidade dessas novas formas de governança mediada por algoritmos. Seja por violar regras de devido processo, concentrar poder decisório nas mãos de grandes corporações,

[28] PRADO, Luis Fernando. **Algoritmos e decisões automatizadas: Buscando conformidade com a LGPD**. Coordenação: PALHARES, Felipe. Estudos sobre Privacidade e Proteção de Dados. São Paulo: Thomson Reuters Brasil. 2021. P. 109.
[29] Ibidem, p. 110.

> ou produzir impactos que tendem a priorizar interesses e visões de mundo de uma elite social e econômica, em detrimento de outras camadas da população. Existe, portanto, uma preocupação de que a delegação de decisões às máquinas levará a uma espécie de "ditadura" dos algoritmos e, consequentemente, das pessoas e corporações que detém o poder de criar e gerir essas tecnologias. Se os algoritmos têm se tornado as "novas leis" da vida *onlife*, mostra-se necessário questionar em que medida esses novos formatos de governança da ordem social são democraticamente legítimos.[30]

Na obra, os autores elaboram críticas à legitimidade da governança mediada por algoritmos, seja por entidades públicas ou privadas. As principais preocupações incluem a violação de regras de devido processo, a concentração de poder decisório em grandes corporações e a priorização dos interesses de uma elite social e econômica, prejudicando outras camadas da população.

Por conseguinte, há um temor de que delegar decisões a máquinas possa resultar em uma verdadeira "ditadura" dos algoritmos, a qual apenas beneficia aqueles que controlam essas tecnologias. Assim, considerando que algoritmos estão se tornando as "novas leis" na era digital, é crucial questionar até que ponto esses formatos de governança são democraticamente legítimos.

Sob tal aspecto, a Academia Brasileira de Ciências, coordenada por Virgílio Augusto Fernandes Almeida, emitiu em novembro de 2023 um relatório com recomendações para o avanço da inteligência artificial no Brasil[31], ressaltando que o desenvolvimento de ferramentas IA é um poderoso avanço da tecnologia, pois impulsiona o crescimento econômico e social do País, sendo fundamental para fomentar descobertas na ciência.

As principais recomendações do Grupo de Trabalho de Inteligência Artificial (GT-IA) da Academia Brasileira de Ciências para o avanço da inteligência artificial no Brasil incluem (i) investimentos significativos e de longo prazo em pesquisa e desenvolvimento de IA, com aumento do financiamento governamental e incentivo para o setor privado[32]; (ii) a valorização da pesquisa e desenvolvimento em IA, com proteção e aumento da força

---

[30] MONTEIRO, Júlia Iunes; MARRAFON, Marco Aurélio. **Legitimidade democrática na governança algorítmica: Primeiros parâmetros para sua aplicação na regulação e no desenvolvimento da inteligência artificial e de políticas baseadas em dados**. Revista Direitos Fundamentais & Democracia V. 29, N. I. jan./abril, 2024. P. 8 e 9. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2747/805

[31] ALMEIDA, Virgílio Augusto Fernandes. **Recomendações para o avanço da inteligência artificial no Brasil**. GT-IA da Academia Brasileira de Ciências. Rio de Janeiro-RJ. 2023. Disponível em: https://www.abc.org.br/evento/doc-ia-no-brasil/

[32] Ibidem, p. 17.

de trabalho nas universidades, facilitação do estabelecimento de marcos regulatórios e legislações que incentivem a comercialização de resultados de pesquisas[33]; e (iii) a formação de uma massa crítica qualificada de profissionais em áreas relacionadas à IA, como aprendizado de máquina e ciência de dados, com a necessidade de desmistificar e informar a sociedade sobre a IA, incluindo a atenção especial à população infantil[34].

Assim, por ter surgido de maneira rápida e acessível, é primordial entender e gerenciar os benefícios e riscos inerentes à inteligência artificial através da adoção de sistemas confiáveis. Dessarte, é fundamental equacionar, então, quanto à essencialidade do papel do Estado frente a modulação e manejo desses dados, devendo ser destacado o uso massivo dos aparelhos inteligentes fomentados por inteligência artificial pela população e pelos poderes estatais.

Neste cenário, segundo Alexandre Morais da Rosa, embora a utilização de algoritmos ajude a reduzir aspectos humanos fundamentais, como o desgaste e o estresse emocional, eles também estão sujeitos ao preconceito estrutural proveniente do sistema jurídico, especialmente considerando a forma como são projetados e configurados:

> É verdade que a utilização de algoritmos contribui para minimizar fatores externos aleatórios tipicamente humanos, tais como cansaço e instabilidade emocional, mas eles também estão sujeitos a vieses estruturais decorrentes do sistema jurídico, da forma como eles são treinados e de sua própria programação. Como visto, ainda que algoritmos como o Word2vec sejam capazes de assimilar, ao menos em parte, o contexto textual de palavras, não se pode afirmar que eles compreendam conceitos da forma como humanos fazem. Sua "compreensão" limita-se a associar uma palavra a outras que geralmente a acompanham e, ainda que se possa chegar a bons resultados através desse método, isso não é o suficiente para dar conta de todas as formas de uso da linguagem, que, assim como o Direito, configura um fenômeno social complexo. Mas se pode falar em possibilidade de "entendimento" e uso supervisionado.[35]

Como visto, embora algoritmos possam reduzir influências humanas aleatórias, como o cansaço e a instabilidade emocional, eles ainda sofrem dos vieses estruturais provenientes das especificidades do sistema jurídico, do treinamento e da programação. Nesse aspecto, embora afirmem os autores que algoritmos como o *Word2vec* podem

[33] Ibidem, p. 15.

[34] Ibidem, p. 14.

[35] BOEING, Daniel Henrique Arruda; ROSA, Alexandre Morais da. **Ensinando um Robô a Julgar. Pragmática, discricionariedade, heurísticas e vieses no uso de aprendizado de máquina no Judiciário**. 1ª Ed. Florianópolis-SC: Emais Academia, 2020. P. 90 e 91.

associar palavras com outras no contexto, isso não significa que eles compreendem conceitos como humanos.

Afinal, é demonstrado que os algoritmos simplesmente fazem associações baseadas em padrões de palavras, o que, conquanto possa produzir bons resultados, não é suficiente para a total compreensão do uso complexo da linguagem, especialmente em áreas como o Direito, de modo que os algoritmos podem ser úteis com supervisão humana, pois sua "compreensão" é limitada.

Não bastasse isso, Luís Greco ressalta que em algumas hipóteses os algoritmos que compõem as inteligências artificiais podem atuar de forma discriminatória:

> Pior: os erros não são distribuídos com base em um princípio aleatório, mas se cometem de forma sistemática em desfavor dos mais fracos. Algoritmos, afirma-se criticamente, operam frequentemente de forma discriminatória: "Eles tendem a punir os pobres". Isso ocorre menos pelo fato de que os algoritmos refletiriam o sistema valorativo de seus criadores, e já pela própria matemática que os fundamenta. Ainda que o programa seja cego em relação a dados "sensíveis", como aqueles que a Constituição Federal brasileira arrola no art. 3 IV ("origem, raça, sexo, cor, idade") - o processamento de uma massa de outros dados, a estes relacionados, faz com que os dados inicialmente desconsiderados, por assim dizer, ressuscitem e se façam perceber nas conclusões, principalmente no nível macro.[36]

O trecho aponta que os erros cometidos por algoritmos não ocorrem de maneira aleatória, mas afetam de forma desproporcional os grupos mais vulneráveis, como os pobres, pois, mesmo que os algoritmos não considerem diretamente informações sensíveis, como raça, sexo ou idade, são utilizados outros dados que, indiretamente, correlacionam-se com essas características[37]. Assim, no processamento de grandes quantidades de dados, esses fatores "escondidos" acabam influenciando os resultados, gerando efeitos discriminatórios.

---

[36] GRECO, Luís**. Poder de julgar sem responsabilidade de julgador: A impossibilidade jurídica do juiz-robô**. São Paulo, SP: Marcial Pons, 2020. P. 29.

[37] "Esse tipo de discriminação (indireta) pode decorrer não apenas de processos irracionais inconscientes, mas também por intermédio de tecnologias de automação, a exemplo do uso de inteligência artificial na contratação de trabalhadores, no monitoramento policial por data mining, data matching ou reconhecimento facial, na concessão de benefícios assistenciais, no direcionamento publicitário e na moderação de conteúdo em redes sociais. Daí decorrem duas importantes questões. A primeira delas consiste em saber como é possível evitar práticas discriminatórias abusivas causadas por novas tecnologias, a exemplo dos algoritmos de machine learning. A segunda consiste em saber se é possível a automatização do processo decisório para fins de identificação de práticas discriminatórias.". LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. 2.ed., rev. e atual. 2 São Paulo: Editora JusPodivm. 2024. P. 286.

Apesar das críticas, é certo afirmar que, à medida que a substituição da voz pensante pela inteligência artificial, do córtex cerebral pela Plataforma Cortex[38] ou do homem pela máquina avança, torna-se necessário o preparo técnico adequado e o amparo legal mínimo para garantir a segurança e a eficácia dessas tecnologias, pois a memória humana foi basicamente substituída por mecanismos digitais através dos históricos armazenados e dados coletados pelo celular, de forma consciente ou não:

> [...] a humanidade está aceitando, paulatinamente, a ideia pós-Turing no sentido de que não somos seres newtonianos ou agentes únicos, mas sim organismos informacionais (*infors*) em um ambiente informacional (*inforsphere*). Essa aceitação decorre da transição da *história* para a *hiper-história* e da dependência em tecnologias da informação e comunicação (ICTs). Nessa nova revolução copernicana, os seres humanos não podem mais ser considerados o centro da infosfera. Isso porque nossas memórias, decisões, tarefas diárias e outras atividades são constantemente delegadas a agentes artificiais.
> Seja como for - estejamos ou não em uma etapa tecnológica essencialmente nova ou em uma continuidade da terceira revolução -, o fato é que, especialmente a partir da década de 2010, os produtos e serviços digitais adentraram fortemente a vida das pessoas.[39]

Não é forçoso lembrar que o *smartwatch* contabiliza passos e a frequência cardíaca; a fechadura eletrônica registra horários de entrada e saída; o *kindle* tem histórico completo de leitura; a *Alexa* conhece a *playlist* musical; o computador os arquivos do ofício laborado armazenado e que todos esses dispositivos, direta ou indiretamente, possuem captação de voz.

Quanto ao *smartphone*, em regra integralmente está conectado a todos os dispositivos inteligentes e a todos os aplicativos utilizados pelo usuário, pois armazena o histórico de navegação, arquivos audiovisuais, mensagens instantâneas, numerários bancários, aplicativos de mídias sociais, *e-commerce*, preferências de filmes/séries em *streaming* e jogos em plataformas digitais.

Aos clientes iFood, por exemplo, a famosa frase que remonta à perda de memória de curto prazo *"não me recordo nem o que almocei ontem"* já não pode mais ser utilizada: basta acessar o histórico de pedidos e lá irá constar a forma de pagamento, o cardápio escolhido, a quantidade, o endereço do consumidor e até o tempo que se transcorreu desde a efetivação do pedido até a respectiva entrega.

---

[38] *Vide:* https://plataforma.cortexai.com.br/users/sign_in

[39] LORDELO, op. cit. p. 85 e 86.

O mesmo ocorre quando se quer lembrar onde, como e com quem esteve em uma data específica, pois os álbuns de recordações dos aparelhos celulares possuem todas essas informações armazenadas na fotografia realizada.

As atribuições das agências bancárias também foram substituídas pelas funcionalidades do celular na mesma proporção, haja vista que o aplicativo bancário confere acesso a toda movimentação financeira do titular em frações de segundos.

O comprovante de um pagamento instantâneo via *pix* com todos os elementos da transação, incluindo dados pessoais do pagador e recebedor, pode ser imediatamente compartilhado via *WhatsApp*, Mídias Sociais e endereço eletrônico.

Todo o conteúdo digital presente em um *smartphone* está conectado a outros dispositivos inteligentes usados pelo indivíduo, e suas bases de dados são armazenadas em plataformas desenvolvidas por empresas como Google, Amazon, Apple, Samsung e Microsoft. Essas empresas, por conseguinte, possuem controle significativo sobre as atividades diárias de todas as pessoas.

Da perspectiva levantada por Shoshana Zuboff, por exemplo, os arquivos de dados angariados pelo termostato Nest são diretamente conectados e enviados aos servidores do *Google*, e que:

> Com um *Wi-Fi* habilitado e conectado, os intricados e personalizados arquivos de dados do termostato são enviados aos servidores do Google. Cada Termostato vem com uma "política de privacidade", um "contrato de termos de serviço" e um "contrato de licença para o usuário final". Esses documentos revelam consequências opressivas para a privacidade e a segurança, nas quais informações sensíveis do indivíduo e da casa são compartilhadas com outros dispositivos inteligentes, departamentos não identificados de empresas e terceiros, para propósitos de análise preditiva e vendas a outras partes não especificadas. A empresa proprietária do *Nest* assume pouca responsabilidade pela segurança da informação que coleta e nenhuma pela maneira como as demais companhias do seu ecossistema farão uso desses dados. Uma análise detalhada das políticas da *Nest Labs* realizada por dois estudiosos da Universidade de Londres concluiu que, se alguém entrasse no ecossistema de dispositivos e aplicativos conectados ao Nest — cada um com termos opressivos e audaciosos próprios —, a aquisição de um único termostato doméstico implicaria a necessidade de rever quase mil dos assim chamados contratos.[40]

O texto descreve como os termostatos inteligentes da Nest, ao serem conectados ao *Wi-Fi*, enviam dados detalhados e personalizados para os servidores do Google.

[40] ZUBOFF, op. cit. P. 17 e 18.

Embora esses dispositivos venham com políticas de privacidade, termos de serviço e contratos de licença, eles têm consequências negativas para a privacidade e segurança dos usuários, pois diversas informações sensíveis sobre os indivíduos e suas casas são compartilhadas com outros dispositivos, departamentos desconhecidos de empresas e terceiros, tudo sob a aparente finalidade de realização de "análises preditivas" e vendas.

Como consequência disso, a empresa responsável pelo termostato assume pouca responsabilidade pela segurança das informações coletadas e também não se responsabiliza por nenhuma das ações das outras empresas em seu ecossistema.

Além do mais, a título de exemplo, em 2016, a Microsoft apresentou a Cortana[41], um tipo de assistente digital pessoal, durante a Conferência Ignite[42] organizada pela empresa. A Cortana foi promovida como uma nova interface centrada no usuário, capaz de conhecê-lo profundamente, incluindo seu contexto, sua família e seu trabalho, sem limitações, e sendo acessível em qualquer dispositivo[43].

Nesse aspecto, o *Google* construiu o sistema *Google Now* (atualmente remodelado como *Google Assistant*), estruturando todas as plataformas criadas até então, de modo a aprender a partir do conteúdo e do comportamento do indivíduo, incluindo seu telefone, movimentos, localização, atividades, voz e aplicativos.

Basicamente, de acordo com a pesquisadora Zuboff, o *software* sabe e até adivinha a informação que o usuário irá precisar em dado momento, de modo que tem ciência sobre que horas é seu voo agendado; se uma encomenda foi entregue; quanto tempo sua cônjuge demorará para chegar em sua residência e onde se encontra; tudo através de processos de plataformas treinadas a partir de fluxos de dados reais e virtuais[44].

Tais dados, por sua vez, usualmente têm sido coletados no âmbito de investigações e instruções processuais penais, sendo utilizados como acervo probatório para culpabilizar indivíduos submetidos ao poder punitivo estatal.

Assim, é evidente que a sociedade contemporânea está profundamente imersa na era digital, onde a tecnologia desempenha um papel central em nossas vidas e a

---

[41] Semelhante à Siri da Apple e à Alexa da Amazon.

[42] Microsoft revela novos recursos que dão poder para TI realizar a transformação digital. 26.09.2016. Microsoft News Center Brasil. Disponível em: https://news.microsoft.com/pt-br/microsoft-revela-novos-recursos-que-empoderam-ti-para-realizar-a-transformacao-digital/

[43] **Satya Nadella: Microsoft Ignite 2016**. 26.09.2016. Disponível em: https://news.microsoft.com/speeches/satya-nadella-microsoft-ignite-2016/

[44] ZUBOFF, op. Cit. P. 382.

dependência tecnológica é cada vez mais notória, refletindo-se não apenas na comunicação cotidiana, mas também na forma de lidar com a persecução penal.

Nessa esteira, a coleta de dados e informações digitais se tornou uma prática comum em investigações criminais, levantando questões éticas e legais sobre a privacidade e a proteção de dados dos indivíduos. Além disso, a evolução tecnológica trouxe consigo a necessidade de adaptação do sistema jurídico, que precisa acompanhar as mudanças para garantir a eficácia das investigações e a proteção dos direitos individuais.

Como será discutido no decorrer desta dissertação, a falta de regulamentação específica sobre o acesso aos dados armazenados em nuvem em investigações criminais destaca a urgência de atualização das leis para lidar com os desafios trazidos pela era digital, de modo que a discussão sobre a proteção da privacidade e a garantia de um processo penal transparente e justo deve ser prioridade na agenda jurídica contemporânea.

Em suma, a análise constitucional sobre a temática da violabilidade dos dados e informações digitais é essencial para assegurar que as medidas adotadas no âmbito da persecução penal estejam em conformidade com os princípios fundamentais estabelecidos pela Constituição da República, pois a proteção dos dados dos cidadãos e a garantia de um processo penal justo e equilibrado são pilares essenciais para a manutenção do Estado de Direito.

2. A PROTEÇÃO E O ACESSO ÀS INFORMAÇÕES E DADOS DIGITAIS DURANTE A PERSECUÇÃO PENAL

Neste tópico, serão analisadas as características da persecução penal sob o enfoque da coleta, do uso e da gestão de dados, especialmente os coletados nas "nuvens" dos aparelhos telefônicos pertencentes às pessoas investigadas, as quais correm risco de tê-los utilizados como prova em eventual investigação criminal.

Serão feitas elucidações fáticas sobre o cenário investigativo nacional, considerando seus costumes, mazelas e efeitos na vida dos indivíduos alvejados por buscas pessoais seguidas de forçado acesso ao conteúdo do aparelho celular, buscas e apreensões, quebras de sigilo telemático e interceptação do fluxo de comunicações em sistemas de informática e telemática, estas últimas recebendo destaque principal.

Dito isto, em primeiro plano, deve ser destacado que, dentre os contornos da persecução penal, é certo que seu desenrolar ocorre tanto na investigação preliminar - na esfera do Inquérito Policial ou do Procedimento Investigatório Criminal - quanto no processo judicial em si, com a efetiva participação dialética das partes.

Apesar disso, no contexto brasileiro, é característica consuetudinária que as provas documentais consideradas não repetíveis (CPP, artigo 155), cuja tendência é se tornarem as bases probatórias de eventual sentença condenatória, são prioritariamente coletadas na fase pré-processual sem a presença do contraditório, restando à defesa na fase judicial tão somente a informação das conclusões obtidas nos documentos produzidos, seja por meio pericial ou lógico-argumentativo, quando então já paira sobre o agente o estigma de ter sido denunciado sob a égide da validade e eficiência dos elementos documentados utilizados para lastrear o oferecimento da denúncia.

Nesse contexto, nos crimes de ação penal pública, a fase inicial, ou investigação preliminar, a qual pode ser conduzida por meio de inquéritos policiais, comissões parlamentares de inquérito ou procedimentos investigatórios criminais, tem incumbência de angariar documentos, depoimentos e demais meios probatórios com a finalidade de compor a *opinio delicti* do Ministério Público, titular da ação penal (CRFB, artigo 129, I).

Na esfera do inquérito policial, a investigação é realizada pela Polícia Judiciária, seja ela Federal ou Civil, a depender da competência previamente estabelecida para o processamento e julgamento do tipo penal investigado, sempre considerando a teoria do juízo aparente.

Em não raras hipóteses, o ato inicial de uma investigação é praticado pela Polícia Militar, encarregada de atuar em caráter preventivo, seja por meio de busca pessoal, veicular ou domiciliar, quando preenchidos os requisitos legais autorizadores, de modo que, havendo hipótese de prisão em flagrante, este será lavrado o auto e posteriormente será instaurada uma investigação formal.

Devem ser ouvidos, no registro de prisão em flagrante, o agente policial que efetuou a prisão, duas testemunhas que presenciaram o fato e a pessoa detida, podendo haver exceções a tal prática, pois, se não houver duas testemunhas presenciais, podem ser ouvidas duas testemunhas que estavam presentes na apresentação do preso. Nesse sentido, confira-se a lição doutrinária de Gustavo Badaró:

> No auto de prisão em flagrante deverão ser ouvidos o condutor, duas testemunhas presenciais e o conduzido (CPP, art. 304, caput). Esta, porém, é a situação normal de auto de prisão em flagrante, que poderá sofrer variações. Se não houver as duas testemunhas presenciais, poderão ser ouvidas duas testemunhas da apresentação do preso (CPP, art. 304, § 2°.).
> As testemunhas de apresentação e as testemunhas presenciais têm finalidades distintas. As testemunhas presenciais depõem sobre o crime que foi praticado e sua autoria. Já as testemunhas de apresentação atestam apenas o fato de alguém ter sido apresentado para a autoridade policial pelo condutor, que afirma ser ele o autor do delito. É óbvio que, do ponto de vista probatório, a primeira situação gera muito mais segurança.[45]

Também nos inquéritos policiais, a Polícia Judiciária atua em conjunto com o Ministério Público, podendo ambos os entes requerer em juízo a decretação de prisões preventivas, buscas e apreensões, quebras de sigilo fiscal e telemático, interceptações telefônicas, dentre outros meios de prova para compor os indícios mínimos de autoria e materialidade requisitados para o oferecimento da denúncia.

A título de exemplo, o artigo 3º da Lei de Interceptações Telefônicas permite que a interceptação seja realizada durante a investigação, podendo ser solicitada pela autoridade policial ou pelo promotor de justiça, conferindo, inclusive, ao próprio juiz o poder de decidir de ofício a respeito[46].

---

[45] BADARÓ, Gustavo Henrique. **Processo Penal**. 9. ed. rev., atual. e ampl. -- São Paulo : Thomson Reuters Brasil, 2021. P. 1623.

[46] PINHEIRO, Juliana Ferreira Soares. **Contornos da cadeia de custódia no âmbito da interceptação telefônica**. 2021. 51 f. — Universidade de Brasília, Brasília, 2021. P. 33. Disponível em: https://bdm.unb.br/handle/10483/29806. Acesso em 04.09.2024

Com isso, a discussão posta em análise busca discorrer sobre os requisitos autorizadores da coleta e da gestão de dados armazenados eletronicamente, por meio da qual se buscará diferenciar uma atuação investigativa legítima da indesejável pescaria probatória (*fishing expedition*), consistente na atividade policial na qual a linha investigativa é excedida, havendo desvio de finalidade que confere mera aparência de legalidade no procedimento de coleta probatória[47].

As consequências de tal prática na persecução penal brasileira podem refletir efeitos desastrosos, pois, do mesmo modo como um domicílio pode ser indevidamente invadido sem prévio comando judicial - ou a partir de decisão mal fundamentada -, os armazenamentos em nuvem dos indivíduos, muitas vezes com informações muito mais sensíveis em relação às que podem ser encontradas no interior de uma residência, são passíveis de invasão por parte de qualquer agente público encarregado de investigar eventual crime.

Sobre tal perigo, é proveitoso conferir a lição doutrinária de Luís Greco e Orlandino Gleizer:

> Como os celulares são objetos que nos acompanham de perto, do banheiro à beirada da cama, o acesso a esses dispositivos permite não apenas o encontro de informações armazenadas, por exemplo, na caixa de e-mails ou em conversa privada em um aplicativo de mensagens instantâneas, como também acesso ao áudio e vídeo de uma relação sexual, de uma discussão íntima e do diálogo com o médico ou com o advogado de defesa. Por meio de uma vigilância online é possível comprometer não apenas a proteção eficiente do núcleo da esfera privada, como também a própria confiança no uso de dispositivos informáticos, que se transformam em objetos de escuta e gravação ambiental.[48]

Ante o exposto, o trecho em destaque aborda a proximidade e a importância dos celulares para os indivíduos, acompanhando-os em todos os momentos, desde o banheiro até a beira da cama. Os autores ressaltam que esses dispositivos armazenam uma grande

---

[47] ÁVILA, Gustavo Noronha de; SILVA, Luís Gustavo Candido. **O fenômeno da pescaria probatória e os mandados de busca e apreensão genéricos nas operações de combate à corrupção da tutela (in)efetiva dos direitos personalíssimos à intimidade e ao sigilo profissional do contador**. Arquivo Jurídico – Revista Jurídica Eletrônica da UFPIISBN 2317-918X – V. 10, n. 2, jul/dez 2023. P. 3. Disponível em: https://revistas.ufpi.br/index.php/raj/article/view/13803/8558. Acesso em 15.07.2024.

[48] GRECO, Luís; GLEIZER, Orlandino. **A infiltração online no processo penal** – Notícia sobre a experiência alemã. Rev. Bras. de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, set.-dez. 2019. P. 1508.

quantidade de informações pessoais, como e-mails, conversas privadas, e até registros de momentos íntimos, como relações sexuais ou discussões confidenciais.

Por conseguinte, com a vigilância online, muitas vezes praticada por órgãos oficiais de investigação criminal, há um risco significativo de comprometer a privacidade dessas informações, transformando os celulares em instrumentos de espionagem e gravação, afetando direitos fundamentais e a confiança dos usuários na segurança desses dispositivos.

Com isso, no primeiro subtópico, serão discutidos os princípios que circundam a coleta e o uso de informações em aparelho telefônico, sendo expostas as possibilidades e limites da investigação, além da comparação da quebra de sigilo telemático com o instituto da interceptação telefônica, bem como a evolução jurisprudencial sobre a matéria.

Ademais, o segundo subtópico discorrerá sobre a Lei 12.965/14 e a jurisprudência brasileira sobre o acesso de dados armazenados eletronicamente, sendo levados em consideração os julgados que se utilizam do Marco Civil da Internet como Legislação Federal aplicável aos casos de quebra de sigilo telemático, mais especificamente no tocante à fundamentação das decisões judiciais que determinam tal medida investigativa.

2.1. Os métodos investigativos e a vigilância policial

A vigilância policial um papel crucial na manutenção da ordem pública e na proteção da sociedade contra atividades criminosas, sendo realizadas por entes estatais com poder de investigação, a exemplo da Polícia Judiciária Civil e da Polícia Federal, podendo contar com o apoio do Ministério Público[49], os quais em conjunto têm a responsabilidade de investigar, prevenir e reprimir crimes, devendo as investigações, em regra, ser objeto de controle do Poder Judiciário.

Nesse aspecto, a eficácia da vigilância para a instauração de operações não depende apenas da ação imediata dos agentes incumbidos dessa função, mas também da aplicação de métodos de investigação bem estruturados, sendo estes fundamentais para

[49] Nesse sentido: "Conclui-se assim que, ao considerar o Ministério Público um órgão estatal comprometido com a garantia e efetivação do compromisso constitucional, bem como estruturado de forma adequada para essa incumbência, tem-se por legítima a sua investigação criminal, diante da necessidade de proteção penalmente efetiva dos direitos fundamentais.". NETO, Mario Azambuja. **Investigação criminal pelo Ministério Público: Para além da questão da (im)possibilidade**. Rev. SJRJ, Rio de Janeiro, v. 17, n. 29, p. 151-174, dez. 2010. P. 166. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/74980 Acesso em 15.07.2024

garantir que as ações investigativas invasivas sejam lastreadas em informações precisas e análises detalhadas, aumentando a probabilidade de sucesso nas operações sem prejuízo das garantias fundamentais da pessoa investigada.

Dessarte, a importância dos métodos de investigação se torna evidente sobretudo diante da complexidade das novas modalidades de crime, porquanto as organizações criminosas frequentemente operam de maneira sofisticada, utilizando tecnologias avançadas e redes de comunicação para evitar a detecção.

Nesse contexto, a simples abordagem reativa das operações policiais já não é suficiente, sendo necessário um planejamento estratégico que envolva a coleta e análise de dados, a identificação de padrões de comportamento criminoso e a antecipação de ações. Métodos como o F3EAD, que combina ações operacionais com inteligência, são exemplos de como a investigação pode ser aprimorada para enfrentar esses desafios. Esse método é assim definido por Daniel Keiny Cardoso e Paulo Alexandre Rodrigues:

> O ciclo "F3EAD" ("Find, Fix, Finish, Exploit, Analyze and Disseminate") ou Encontrar, corrigir, finalizar, explorar, analisar e disseminar), metodologia desenvolvida por forças militares norte-americanas para a integração de atividades operacionais de campo e de inteligência, tem como foco o processamento objetivo das informações colhidas em campo, para tomada imediata de decisões e busca de novos alvos.
> "F3EAD" é um sistema que permite ao operador das forças especiais antecipar e prever operações criminosas, identificar, localizar e realizar exploração e análise de inteligência de pessoal e material apreendidos. O ponto central do process o "F3EAD" é a fusão funcional das operações e funções de inteligência em toda a organização de operações especiais. No "F3EAD", os comandantes estabelecem as prioridades de seleção de alvos, o sistema de inteligência fornece as informações atinentes ao caso e as forças especiais executam as operações decisivas necessárias para cumprir a missão. Tudo se destina a produzir informações objetivas e no menor tempo possível.
> Ao contrário de outros modelos e processos de segmentação tradicionais, que se concentram no aspecto operacional, o principal esforço do "F3EAD"é a inteligência, especialmente a parte "pesquisar-analisar-divulgar". O processo "F3EAD" funciona como uma rede onde os vários elementos do processo trabalham em conjunto, ligados diretamente uns aos outros ou a uma fusão de operações e sistemas de inteligência.[50]

Como visto, o ciclo "F3EAD" (Encontrar, Corrigir, Finalizar, Explorar, Analisar e Disseminar) é uma metodologia desenvolvida pelas forças militares norte-americanas para integrar atividades operacionais de campo e de inteligência. Esse processo se

[50] CARDOSO, Daniel Keiny; RODRIGUES, Paulo Alexandre. **O emprego do operador de operações especiais em conjunto com o agente de inteligência**. Brazilian Journal of Development, *[S. l.]*, v. 9, n. 6, p. 20481–20494, 2023. DOI: 10.34117/bjdv9n6-114. P. 20488. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/60865. Acesso em 18.07.2024

concentra no uso eficiente das informações coletadas no campo para tomar decisões rápidas e identificar novos alvos, permitindo que os operadores das forças especiais antecipem e previnam operações criminosas, além de identificar, localizar, explorar e analisar a inteligência obtida de pessoas e materiais apreendidos.

Aponta o texto referenciado que o ponto central do "F3EAD" é a fusão das operações com as funções de inteligência dentro da organização de operações especiais. A partir disso, os comandantes definem as prioridades de seleção de alvos, a inteligência fornece as informações relevantes e as forças especiais executam as ações necessárias para cumprir a missão, tudo com a finalidade de produzir informações objetivas o mais rapidamente possível.

Diferente de outros modelos tradicionais que focam no aspecto operacional, o "F3EAD" dá maior ênfase à inteligência, especialmente nas etapas de pesquisa, análise e divulgação, funcionando como uma rede onde todos os elementos trabalham juntos, interligados diretamente ou por meio de uma fusão de operações e sistemas de inteligência.

Além disso, a utilização de outros métodos de investigação adequados permite que as operações policiais sejam mais proativas do que reativas. Isso significa que, ao invés de apenas responder a crimes já cometidos, as forças de segurança podem trabalhar para prevenir a ocorrência de novos delitos. Com isso, a análise de informações e a produção de conhecimento sobre o crime são essenciais para identificar tendências e ameaças, possibilitando a implementação de medidas preventivas.

Por conseguinte, a inteligência artificial emerge como uma ferramenta poderosa que potencializa as capacidades do método F3EAD, podendo processar grandes volumes de dados de forma rápida e eficiente, permitindo que as forças de segurança analisem informações coletadas em tempo real.

Nesse contexto, é imperioso ressaltar que tal método investigativo pode se valer de diversos instrumentos invasivos. Dentre tais mecanismos, os *spywares* vêm ganhando destaque nos últimos anos. Acerca dos perigos decorrentes das funcionalidades dos *spywares*, lecionam as professoras Maíra Fernandes e Carina Quito:

> *Spywares* como o Pegasus são comparados a armas digitais, porque invadem dispositivos informáticos sem qualquer ação do usuário, permitindo acesso amplo e oculto a dados armazenados, monitoramento de todas as atividades e ganho de controle sobre as funcionalidades do aparelho. À distância, o software pode realizar qualquer função: abrir

> microfone e câmera, visualizar ou apagar arquivos, fotos, contatos, localização, acessar aplicativos e dados bancários.
> Não bastasse, o spyware pode se autodestruir sem deixar qualquer vestígio no aparelho no qual foi introduzido à distância. Essa potencialidade é particularmente relevante no debate sobre seu uso na persecução penal, pois é impossível assegurar a cadeia de custódia da prova extraída por esse tipo de ferramenta.
> O uso indiscriminado de softwares maliciosos também preocupa sob o ponto de vista da cibersegurança e da própria soberania nacional. Em regra, essas tecnologias são estrangeiras e comercializadas por empresas privadas que desenvolvem suas atividades de forma opaca, lucrando com a exploração de vulnerabilidades em dispositivos, sistemas e redes de comunicação.[51]

Como visto, o trecho compara *spywares* como o *Pegasus* a armas digitais, destacando que esses programas invadem dispositivos sem o conhecimento do usuário, permitindo acesso total e escondido a dados e controle do aparelho, podendo executar diversas funções remotamente, como ativar microfone e câmera, visualizar e apagar arquivos, acessar dados bancários, entre outros.

Além disso, o *spyware* pode se autodestruir sem deixar rastros, o que complica a preservação da prova em contextos criminais, de modo que o uso generalizado desses *softwares* levanta preocupações sobre a cibersegurança e a soberania nacional, já que são desenvolvidos por empresas privadas estrangeiras que lucram explorando vulnerabilidades tecnológicas.

Consequentemente, tendo em vista o potencial nocivo desses novos *softwares* que utilizam Inteligência Artificial, Felipe Giacomolli alerta sobre o risco gerado pelo policiamento discriminatório exercido com auxílio desses algoritmos:

> Diante desse contexto, analisando o uso de *softwares* de policiamento preditivo na realidade brasileira e considerando que esses sistemas são dotados de algoritmos baseados em Inteligência Artificial construídos para identificar e delinear padrões de criminalidade para alcançar um resultado probabilístico sobre um evento futuro, mostra-se considerável o risco da perpetuação de um policiamento discriminatório, evidenciada sob dois ângulos distintos: 1) banco de dados policiais utilizado pelo sistema carregado de vieses sistêmicos e estruturais de uma polícia profundamente tendenciosa; 2) pela forma como o *software* é construído

[51] FERNANDES, Maíra. QUITO, Carina. **Riscos do uso de *softwares* espiões em atividades de persecução criminal e de inteligência**. Conjur. 12.06.2024. Disponível em: https://www.conjur.com.br/2024-jun-12/riscos-do-uso-de-softwares-espioes-em-atividades-de-persecucao-criminal-e-de-inteligencia/. Acesso em 15.06.2024

> e modelado - quais variáveis, conexões e parâmetros são utilizados e priorizados.[52]

O trecho mencionado critica o uso de *softwares* de policiamento preditivo no Brasil, notadamente os que utilizam algoritmos de Inteligência Artificial para identificar padrões de criminalidade e prever eventos futuros. É evidenciado um risco significativo de perpetuação de práticas de policiamento discriminatórias, o que pode se dar tanto pelos bancos de dados policiais usados pelos sistemas, os quais são passíveis de contaminação por preconceitos ou discriminações históricas e estruturais dentro das forças policiais, quanto pela forma como os algoritmos são desenvolvidos.

Por outro lado, acerca dos benefícios do uso de programas invasores, confira-se a seguinte lição doutrinária:

> A utilização de *malwares* em atividades investigativas é reivindicada sobretudo pelo elevado grau de eficiência que eles podem oferecer, ainda mais por se valer de um cenário de crescente integração de mecanismos informáticos ao cotidiano dos indivíduos e da utilização dos meios digitais para a prática de delitos. A diversidade e extensão dos dados e informações possíveis de serem acessados permite a eles alcançarem resultados superiores àqueles que seriam obtidos pelos meios tradicionais de obtenção de prova. De fato, tais softwares viabilizam o acesso a elementos que dificilmente poderiam ser acessados por outras vias, permitindo inclusive o drible de mecanismos que elidem o acesso a informações contidas em sistemas informáticos, tais como a criptografia ou a dissimulação do IP do computador de onde a comunicação é realizada.[53]

Outrossim, a título de exemplo, algoritmos de aprendizado de máquina podem identificar padrões e anomalias em dados de comunicação, movimentações financeiras e atividades suspeitas, facilitando a localização de alvos e a antecipação de ações criminosas, sendo capacidade de análise preditiva fundamental para a fase de "Encontrar" do ciclo F3EAD, onde a identificação de alvos se torna mais precisa e fundamentada.

---

[52] GIACOMOLLI, Felipe. **Gerenciamento Tecnológico do Sistema de Justiça Penal: As novas tecnologias no âmbito do policiamento, da investigação e da decisão**. 1. Ed. Rio de Janeiro: Marcial Pons. 2023. P. 137.

[53] RIBEIRO, Gustavo A. M.; CORDEIRO, Pedro Ivo R. V.; FUMACH, Débora M. **O *malware* como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro**. Revista Brasileira de Direito Processual Penal, vol. 8, n. 3, p. 1463-1500, set./dez. 2022. Disponível em: https://doi.org/10.22197/rbdpp.v8i3.723. Acesso em 25.07.2024

Além disso, a IA pode aprimorar a etapa de "Analisar"[54] ao fornecer *insights* que seriam difíceis de obter por métodos tradicionais, podendo as ferramentas de análise de dados baseadas em IA cruzar informações de diversas fontes, como redes sociais, registros públicos e dados de vigilância para criar um panorama mais completo das atividades criminosas.

A inteligência artificial se torna um aliado indispensável na busca por informações relevantes que sustentem as operações, não apenas complementando, mas também transformando a abordagem do F3EAD, elevando a eficácia das operações policiais e contribuindo para um combate mais eficiente ao crime, podendo ser utilizada tanto nas operações comuns quanto nas de grande porte.

Uma operação comum e uma megaoperação se diferenciam principalmente em escala, complexidade e recursos mobilizados. Em primeiro plano, uma operação comum geralmente envolve investigações mais simples, com um número limitado de policiais e focada em um único local ou em um grupo restrito de suspeitos. Estas operações podem ser reativas, respondendo a um crime específico ou a uma notícia de fato, sendo de costume a utilização de técnicas investigativas tradicionais.

Por outro lado, uma megaoperação é caracterizada por sua grande escala e abrangência, envolvendo uma equipe diversificada de policiais, muitas vezes de diferentes estados ou até países, e lida com alvos que operam em múltiplos locais, sendo planejadas para desmantelar organizações criminosas complexas, com grande poder econômico e social, frequentemente requerendo o uso de técnicas investigativas avançadas, como interceptação telefônica e cooperação internacional.

Além disso, elas podem resultar em ações simultâneas em diversos locais, com a mobilização de dezenas ou centenas de policiais, geralmente incluindo prisões em massa e apreensões significativas de bens e valores.

As grandes operações são assim definidas pelo professor Célio Jacinto dos Santos:

> Investigações que demandam bom tempo de trabalhos de levantamento de informações; Com equipe composta por diversos policiais; Envolvendo alvos em diversos locais (estados ou países); Cujas ações criminosas são diversificas no tempo e espaço; Detenha grande poderio econômico, social, político; Requeira emprego de técnicas mais apuradas de investigação; Que permita a deflagração concomitante em diversos

[54] "Analyze" - Analisar: fundir a evidência explorada com o quadro de inteligência mais amplo. No "analisar" as informações obtidas na fase de localizar, consertar, aumentar e investigar são transformadas em inteligência que pode ser usada para orientar as operações.". CARDOSO; RODRIGUES, op. cit. P. 20489.

> locais, com dezenas ou centenas de policiais; Com prisões e apreensão de bens, valores, instrumentos, veículos etc.; Quase sempre com emprego de cooperação policial estrangeira ou cooperação de outro órgão de controle.[55]

Conforme exposto, as megaoperações são investigações complexas que exigem um longo período de coleta de informações, sendo realizadas por equipes compostas por diversos policiais, cujos esforços visam a alvos espalhados por diferentes locais, seja em estados ou países.

No âmbito das megaoperações, diversas são as técnicas investigativas que podem ser utilizadas com a finalidade de auxiliar na apuração de eventuais práticas criminosas. Em primeiro lugar, as *ações encobertas* são uma das técnicas mais eficazes utilizadas pelas autoridades policiais, consistindo na infiltração de agentes de polícia em grupos criminosos, permitindo a coleta de informações valiosas sobre suas operações e estruturas, sendo tal técnica fundamental para desmantelar organizações criminosas, possibilitando a obtenção de provas que, de outra forma, seriam inacessíveis.

No âmbito brasileiro, o instituto do agente infiltrado é tutelado pelos artigos 10 a 14 da Lei 12.850/13, estando fixado que a infiltração só pode ocorrer mediante autorização judicial detalhada, que define os limites e a duração da operação, sendo imprescindível a presença de indícios claros de infração penal que não possam ser provados por outros meios disponíveis.

Conforme preconiza a doutrina de Marco Ribeiro Henriques, a infiltração não apenas ajuda na coleta de dados, mas também na identificação de líderes e na compreensão das dinâmicas internas do crime organizado:

> No que à infiltração diz respeito, e numa orientação sintomática da cada vez maior preocupação com a eficácia da justiça criminal, a doutrina tende a convergir no entendimento uno, porquanto seja admissível o recurso a esta técnica especial de investigação em situações limite ou excecionais, nomeadamente quando os restantes meios de investigação à disposição das instâncias formais de controlo se mostram insuficientes para afrontar com sucesso a atividade dos criminosos e que a criminalidade ponha gravemente em causa os valores fundamentais que à Justiça criminal cabe tutelar.[56]

---

[55] SANTOS, Célio Jacinto dos. **A gênese das grandes operações investigativas da polícia federal**. Revista Brasileira de Ciências Policiais. Brasília, v. 8, n. 2, p. 9-66, jul/dez 2017. P. 17. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/526/309 Acesso em 26.08.2024

[56] HENRIQUES, Marco Ribeiro. **Ações encobertas, para fins de investigação criminal. A dicotomia entre agente infiltrado e agente provocador**. Revista Jurídica UNIGRAN. Dourados, MS | v. 18 | n. 34 | Jan./Jun.2016. P. 99. Disponível em:

Outra técnica relevante é o acordo de colaboração premiada, também conhecida como delação premiada[57], que é um instrumento jurídico que permite a um investigado colaborar com o Ministério Público em troca de benefícios, como a redução da pena ou até mesmo a extinção da punibilidade. Essa prática, regulamentada pela Lei 12.850/13, apresenta características que a tornam um tema controverso no âmbito do direito penal.

Uma das principais características da colaboração premiada é a sua estrutura em três fases: negociação e acordo, homologação judicial e sentença. Tal sistemática busca garantir que o processo de colaboração seja formalizado e supervisionado, evitando a prática de abusos.

No entanto, alguns ramos doutrinários defendem a tese de que o acordo de colaboração premiada viola o princípio da paridade de armas ao conferir à acusação poderes desproporcionais em relação aos delatados. Confira-se a lição de Guilherme Brenner Lucchesi e Lucas Gandolfi Vida:

> Em nome do aprimoramento das técnicas de investigação de crimes imputados a organizações criminosas, tem se admitido a obtenção de provas por métodos ocultos — como é o caso da colaboração premiada —, que aumentam a disparidade na capacidade investigativa das partes. Isto representa (ainda) maior desequilíbrio na paridade de armas entre a atuação defensiva e a acusatória, pois a acusação passa a dispor de mecanismos muito mais amplos e efetivos de investigação. Dada a natureza própria inquisitória dos procedimentos investigativos, demonstra-se um campo de preocupação baseado na possibilidade da inserção de provas ilícitas ou inutilizáveis no processo.[58]

Apesar disso, a colaboração premiada é vista como uma ferramenta eficaz no combate ao crime organizado, pois permite que os delatores forneçam informações valiosas sobre a atuação de grupos criminosos, contribuindo para a elucidação de crimes e a responsabilização de outros envolvidos.

---

https://www.researchgate.net/publication/309618668_Acoes_encobertas_para_fins_de_investigacao_criminal_A_dicotomia_entre_Agente_Infiltrado_e_Agente_Provocador Acesso em 26.09.2024

[57] "O ordenamento jurídico brasileiro apresenta disciplinas jurídicas específicas, em variados diplomas legais, sobre a "colaboração premiada", vulgarmente conhecida como "delação premiada".". BADARÓ, op. cit. p. 723.

[58] LUCCHESI, Guilherme Brenner; VIDA, Lucas Gandolfi. **Perspectivas quanto à lavagem de provas na colaboração premiada: proposta para controle de abuso processual**. Revista Brasileira de Direito Processual Penal, *[S. l.]*, v. 7, n. 3, p. 2203, 2021. Disponível em: https://doi.org/10.22197/rbdpp.v7i3.542 Acesso em Acesso em 20.09.2024

Entretanto, a colaboração premiada também enfrenta críticas significativas. Uma de suas principais preocupações é a possibilidade de que a delação possa ser utilizada como um meio de chantagem ou manipulação, principalmente nos casos em que a delação é utilizada como moeda de troca em favor de delatores presos, onde estes podem ser incentivados a incriminar outros em troca de benefícios pessoais, podendo comprometer o direito à presunção de inocência e transformar o processo penal em um jogo de interesses, podendo a verdade dos fatos ser distorcida em função de acordos entre as partes.

Além disso, a legislação sobre a colaboração premiada é considerada insuficiente em alguns aspectos, especialmente no que diz respeito à proteção dos direitos dos delatados, pois a falta de regras claras sobre como esses indivíduos podem se defender e contestar as declarações dos colaboradores pode levar a um desequilíbrio processual, prejudicando a ampla defesa:

> Até então, o legislador se limitava a tratar dos efeitos materiais, em termos de redução de pena, substituição de pena ou mesmo de extinção da punibilidade que a delação premiada terá. Porém, a disciplina legal da colaboração premiada ainda é muito mais voltada para o conteúdo do acordo de colaboração premiada em si, do que para a forma processual de produção de tal prova e, principalmente, de como os delatados poderão exercer o seu direito à prova em face do delator.[59]

O trecho citado indica que, inicialmente, a legislação sobre a delação premiada focava principalmente nos benefícios materiais concedidos ao delator, como a redução ou substituição da pena, ou até mesmo a extinção da punibilidade. No entanto, a regulamentação legal da colaboração premiada pela Lei 12.850/13 se concentra mais no conteúdo do acordo em si, significando que há maior ênfase em definir os termos e condições do acordo de delação premiada, do que em detalhar os procedimentos processuais para a produção da prova obtida por meio da delação.

Feitas essas considerações, ainda vale destacar que a ação controlada é outra técnica investigativa importante prevista em Lei (artigos 8º e 9º da Lei 12.850/13; artigo 2º, II, da Lei 9.034/95; artigo 33, II, da Lei 10.409/02 e artigo 53, II, da Lei 11.343/06), sendo comumente utilizadas pelas autoridades para rastrear a entrega de substâncias ou objetos ilícitos com a finalidade de capturar criminosos em flagrante postergado. Nesse sentido:

[59] BADARÓ, op. Cit. p. 724.

> A ação controlada é um meio de investigação existente em leis de diversos países e encontra previsão na Convenção de Palermo (arts. 2º e 20), na Convenção de Viena sobre o tráfico ilícito de entorpecentes e, de forma análoga, na Convenção das Nações Unidas contra a corrupção e na Convenção Interamericana contra o Tráfico de Armas. Também é conhecida por "entrega vigiada".
> No Brasil, antes da Lei n. 12.850/13, a ação controlada era prevista no art. 2º, II, na Lei 9.034/95, no art. 33, II da Lei n. 10.409/02 e no art. 53, II da Lei de Drogas n. 11.343/2006. [...] A ação controlada ocorre quando o agente público aguarda o momento oportuno para atuar, a fim de obter, com esse retardamento, um resultado mais eficaz em sua diligência.[60]

Nos termos do trecho mencionado, a ação controlada é uma técnica de investigação usada em várias legislações ao redor do mundo, sendo prevista em convenções internacionais como a de Palermo e a de Viena. Essa prática, também chamada de "entrega vigiada", permite que as autoridades retardem a intervenção imediata em atividades criminosas, aguardando o momento certo para agir com a finalidade de obter melhores resultados.

No Brasil, antes da Lei 12.850/13, esse método investigativo já era regulado por outras leis específicas, como a Lei 11.343/06, que prevê, em seu artigo 53, II, "a não-atuação policial sobre os portadores de drogas, [...] com a finalidade de identificar e responsabilizar maior número de integrantes de operações de tráfico e distribuição, sem prejuízo da ação penal cabível".

Por conseguinte, o objetivo principal da ação controlada é permitir que os agentes públicos coletem provas de maneira mais eficaz por meio do retardamento da ação policial até que se tenha um cenário mais favorável para o sucesso da investigação.

Mais especificamente, a ação controlada é uma técnica especial de investigação que permite retardar a intervenção policial ou administrativa em ações de organizações criminosas, mantendo-as sob vigilância até o momento mais oportuno para a coleta de provas e informações, fazendo jus ao instituto do flagrante esperado[61].

---

[60] BORGES, Amanda Tavares; CARDOSO, Priscila Mara Garcia. **Segurança pública e organizações criminosas no Brasil: Uma análise das ferramentas de investigação utilizadas pela Polícia Civil do Estado de São Paulo**. Revista de Movimentos Sociais e Conflitos | e-ISSN: 2525-9830 | Encontro Virtual | v. 6 | n. 2 | p. 42 - 60 | Jul/Dez. 2020. P. 52. https://doi.org/10.26668/IndexLawJournals/2525-9830/2020.v6i2.7181 Acesso em 16.10.2024

[61] "O flagrante provocado ou preparado não se confunde com o flagrante esperado. Neste, diante da notícia de que um crime poderá ser praticado, a polícia toma as providências para prender em flagrante aquele que irá cometer o crime. O relevante para distingui-lo do flagrante provocado é que, no flagrante esperado, a polícia vigia o local do crime, esperando que o agente, espontaneamente, pratique o delito. Não há induzimento ou provocação para a prática delitiva.". BADARÓ op. cit. P. 1620.

Primeiramente, ao adiar a intervenção, os agentes encarregados pela investigação podem obter uma quantidade maior de provas e informações, o que aumenta a eficácia da ação legal subsequente, permitindo um planejamento mais detalhado e maior compreensão da estrutura e operação da organização criminosa, facilitando a desarticulação de toda a rede de criminalidade.

Como requisitos, no âmbito da Lei de Organização Criminosa (LOA), a ação controlada exige comunicação prévia ao juiz competente (artigo 8º, § 2º, da Lei 12.850/13), que pode estabelecer limites à diligência e informar ao Ministério Público (artigo 8º, § 1º, da Lei 12.850/13). Ao término da diligência, é elaborado um auto circunstanciado, documentando todas as ações realizadas, tendo como finalidade garantir transparência e fornece uma base sólida para eventuais procedimentos judiciais (artigo 8º, § 4º, da Lei 12.850/13).

Quando a ação controlada envolver transposição de fronteiras, a cooperação com autoridades estrangeiras é fundamental para minimizar riscos e assegurar a eficácia da operação internacionalmente, contribuindo para impedir a fuga dos suspeitos e a perda de produtos do crime (artigo 9º da Lei 12.850/13).

Tal modalidade investigativa é frequentemente utilizada em casos de tráfico de drogas, permitindo que a polícia desarticule redes de distribuição e identifique os responsáveis pela logística do crime.

Outrossim, a Lei 9.296/96 estabelece o instituto da interceptação telefônica[62] como modalidade investigativa, sendo rigorosamente regulada pela legislação para garantir sua utilização apenas em situações de real necessidade e com o devido respaldo legal.

Conforme a Lei 9.296/96, a interceptação depende de autorização judicial e deve ocorrer sob segredo de justiça, assegurando a confidencialidade das informações obtidas. Para que a interceptação seja autorizada, é essencial que existem indícios razoáveis de autoria ou participação em um crime, caso contrário - ou se a prova puder ser obtida por outros meios -, a interceptação é vedada.

Ademais, a interceptação não é permitida em casos de crimes punidos apenas com pena de detenção (artigo 2º, III, da Lei 9.296/96), além de que o pedido de interceptação deve ser justificado com clareza pela autoridade policial ou pelo representante do

[62] "A interceptação das comunicações telefônicas é um meio de obtenção de prova típico no ordenamento jurídico brasileiro. Com o advento da Lei 9.296/1996, há mais de vinte anos, foi regulamentada a restrição ao sigilo das comunicações. Ao longo desse período, a tecnologia se modificou e a lei começou a ficar datada, apresentando pontos defasados e omissos.". SMANIO, Gianluca Martins. **Vigilância policial em meio digital: Entre o garantismo e a eficiência**. Curitiba: Juruá, 2022. P. 130.

Ministério Público, detalhando a situação investigada e os indivíduos envolvidos (artigo 2º, parágrafo único, da Lei 9.296/96).

Caso autorizada, a execução da interceptação é minuciosamente monitorada pelo magistrado e pelo Ministério Público, com prazos definidos e a possibilidade de renovação se necessário, mediante requerimento. Ao final, estipula a legislação que todos os procedimentos deverão ser documentados e realizados de forma a garantir a legalidade e a integridade das provas obtidas, preservando sempre a cadeia de custódia e o sigilo das informações.

Por fim, como uma alternativa à interceptação telefônica, a vigilância eletrônica, que inclui o monitoramento por meio de dispositivos tecnológicos, é um método que se tornou indispensável na investigação criminal moderna. Tal técnica investigativa pode envolver o simples espelhamento de aplicativos de comunicação - após a apreensão do aparelho celular -, como também a utilização de *softwares* maliciosos - ou *malwares* - capazes de invadir determinado aparelho eletrônico sem necessidade de apreensão.

A título de exemplo, o termo *malware* contém as tecnologias de vírus, *worms*, *bots*, *trojans*, *spyware*, *backdoor* e *rootkit*. Dentre as principais características de tais espécies de *malwares*, a Cartilha de Segurança para Internet versão 4.0 do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[63] assim as descreve:

Vírus: Um programa malicioso que se propaga inserindo cópias de si mesmo em outros programas e arquivos, dependendo da execução do programa hospedeiro para se tornar ativo. Pode realizar atividades sem o conhecimento do usuário e se propagar por meio de mídias removíveis, como *pen-drives*. [64]

Worm (Verme): Um tipo de *malware* que se replica para se espalhar para outros computadores, muitas vezes explorando vulnerabilidades de rede. Pode se propagar automaticamente pela rede, por e-mail e por outros meios.[65]

Bot e *botnet*: Um programa malicioso que pode ser controlado remotamente para realizar diversas atividades, como enviar *spam*, realizar ataques DDoS (negação de serviço distribuída) e roubar informações.[66]

---

[63] **Cartilha de Segurança para Internet, versão 4.0**. CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/fasciculos/

[64] Ibidem, p. 24.

[65] Ibidem, p. 25.

[66] Ibidem, p. 26.

Trojan (Cavalo de Troia): Um tipo de *malware* que se disfarça como um programa legítimo para enganar os usuários e executar ações maliciosas, como roubo de informações confidenciais ou permitir o acesso remoto ao computador.[67]

Spyware: Um *software* malicioso projetado para coletar informações sobre as atividades do usuário sem o seu conhecimento, como dados de navegação na internet, senhas e informações pessoais.[68]

Backdoor (Porta dos Fundos): Uma vulnerabilidade intencionalmente criada em um sistema para permitir o acesso não autorizado posteriormente. Pode ser usado por invasores para controlar o sistema remotamente.[69]

Rootkit: Um tipo de malware projetado para ocultar a presença de outros *malwares* ou atividades maliciosas no sistema, tornando-se difícil de detectar e remover.[70]

Especificamente acerca do *spyware*, este pode ser definido como um tipo específico de *malware* projetado para espionar as atividades do usuário. Ele coleta informações como hábitos de navegação, dados pessoais e outras atividades sem o conhecimento ou consentimento do usuário, tendo como objetivo monitorar e roubar informações, diferentemente de outros tipos de *malware* que podem ter como objetivo principal causar danos diretos ao sistema.

Resumidamente, enquanto o *malware* é um termo abrangente para todos os tipos de *softwares* maliciosos, o *spyware* é uma subcategoria de *malware* focada na espionagem e coleta de dados do usuário. Assim, as tecnologias de espionagem, como o famoso *software Pegasus*[71], são capazes de coletar informações detalhadas de dispositivos eletrônicos, o que pode ser utilizado para fins de segurança nacional e combate ao crime.

No entanto, o uso dessas tecnologias levanta questões significativas sobre privacidade, direitos humanos e a legalidade de sua aplicação. Sobre o tema, assim leciona Andreia Filipa Santos Duarte:

> Uma vez instalado, o *malware* pode levar a cabo um conjunto de medidas para permanecer indetetável, podendo, simultaneamente, empreender uma panóplia de tarefas tendo em conta aquilo que o atacante pretende que ele faça, possibilitando a recolha de informação interna ao sistema (dados armazenados, não armazenados ou produzidos em tempo real), bem como a recolha de informação externa (através da ativação da

[67] Ibidem, p. 28.
[68] Ibidem, p. 27.
[69] Ibidem, p. 28.
[70] Ibidem, p. 29.
[71] Disponível em: https://www.pegasus.co.uk

> webcam e/ou do microfone). A sua execução pode incluir a comunicação destes dados a uma entidade externa (OPC ou AJ) tendo em vista o seu controlo.
> Posto isto, coloca-se a questão de saber por que razão a utilização de *malware* como meio de obtenção de prova pode revelar-se útil e/ou necessária ao ponto de merecer a sua previsão legal, uma vez que as entidades responsáveis pela investigação criminal têm ao seu dispor, na nossa legislação processual penal atualmente em vigor, um vasto leque de opções no que diz respeito à recolha de prova.[72]

A capacidade de monitorar atividades suspeitas e prevenir crimes é um grande benefício do uso do *spyware* nas investigações criminais. A espionagem pode ser usada para rastrear atividades de organizações terroristas, interceptar comunicações entre criminosos e desmantelar redes de tráfico de drogas, o que torna tais mecanismos essenciais para a segurança pública e a proteção dos cidadãos.

Nesse aspecto, o uso de *spywares* pelos agentes encarregados pela investigação criminal pode acelerar as investigações e fornecer evidências importantes em casos judiciais complexos, pois a capacidade de obter provas digitais de forma rápida e discreta pode ajudar a resolver processos judiciais e garantir que a justiça seja feita de forma eficaz.

Por outro lado, o uso de *spyware* também apresenta sérios riscos, especialmente no que diz respeito à violação da privacidade. Afinal, a coleta indiscriminada de dados pessoais sem o devido processo legal pode levar a abusos e à vigilância em massa, comprometendo os direitos individuais dos cidadãos[73].

Com o avanço da tecnologia, a capacidade de monitorar atividades suspeitas em tempo real permite que as autoridades ajam de forma proativa, prevenindo crimes antes que eles ocorram, porquanto a vigilância eletrônica não apenas fornece evidências concretas, mas também ajuda na análise de padrões de comportamento criminoso.

Assim, no subtópico seguinte, será analisado com mais detalhes a problemática da coleta e do uso de informações em nuvem nos aparelhos celulares pelos agentes encarregados pela investigação criminal.

---

[72] DUARTE, Andreia Filipa Santos. **O malware como meio de obtenção de prova em processo penal.** Repositório científico da UC. Coimbra, 2022. P. 12 e 13. Disponível em: https://hdl.handle.net/10316/103589

[73] HUREL, Louise Marie; FRANCISCO, Pedro Augusto P. TELES, Daisy. **Pegasus, a ponta do iceberg da fragilidade no controle de inteligência e uso de tecnologias de vigilância**. El País. 02.08.2021. Disponível em: https://brasil.elpais.com/opiniao/2021-08-02/pegasus-a-ponta-do-iceberg-da-fragilidade-no-controle-de-atividades-de-inteligencia-e-uso-de-tecnologias-de-vigilancia.html Acesso em 26.10.2024

2.2. A coleta e o uso de dados armazenados na nuvem do investigado

Em primeiro plano, deve-se ter em mente que a fase da coleta de dados na investigação criminal, especialmente no que diz respeito aos arquivos armazenados em nuvem, é um aspecto crucial para a condução de investigações no contexto da era pós-moderna. Essa fase é regida por princípios legais e constitucionais que visam garantir a proteção dos direitos fundamentais dos indivíduos, ao mesmo tempo em que possibilitam a efetividade da justiça criminal[74].

Nesse contexto, alguns métodos de investigação clássicos, a exemplo da busca e apreensão domiciliar, são procedimentos que permitem às autoridades policiais acessarem e coletarem objetos, documentos e informações que possam ser relevantes para a investigação de um crime, oportunidade na qual é aberta uma exceção ao direito fundamental à inviolabilidade domiciliar previsto no artigo 5º, XI, da Constituição da República[75].

De acordo com o Código de Processo Penal, em regra, a busca e apreensão em domicílio deve ser autorizada por um juiz mediante expedição de mandado judicial (artigo 243 do CPP), salvo em situações de flagrante delito, nas quais a urgência da ação pode justificar a ausência de uma ordem judicial prévia (artigo 240, § 1º, do CPP).

Acerca do *standard* probatório necessário para a busca domiciliar sem mandado judicial, confira-se a lição doutrinária de Leandro Lara Moreira:

> A busca domiciliar deve estar previamente legitimada pela prova colhida e não ser o primeiro instrumento utilizado. Para Controle da observância desse requisito, a fundamentação da decisão judicial é o segundo ponto a ser destacado". Neste sentido, a entrada forçada em domicílio sem mandado judicial só é lícita, portanto, quando amparado em fundadas razões, devidamente justificadas a posteriori, que indiquem que, dentro da casa, havia situação de flagrante delito, sob pena de responsabilidade disciplinar, civil e penal do agente ou autoridade, e de nulidade dos atos

[74] "[...] a utilização desses métodos de vigilância em meio digital pela autoridade policial, no contexto da persecução penal, precisa respeitar certos limites constitucionais e legais, de sorte que, para ser eficiente, não pode restringir sem respaldo jurídico os direitos fundamentais do cidadão, sob pena de suprimi-los e desrespeitar a provisão constitucional. Nesta senda, é preciso que exista equilíbrio entre o respeito aos direitos do cidadão e a possibilidade de restringi-los, sempre seguindo ditames constitucionais, legais e jurisdicionais.". SMANIO, Gianluca Martins. **Vigilância policial em meio digital: Entre o garantismo e a eficiência**. Curitiba: Juruá, 2022. P. 16.

[75] "Art. 5º. XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;". BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

> praticados. Deve haver um controle a posteriori, exigindo-se dos agentes estatais a demonstração de que a medida fora adotada mediante justa causa, ou seja, que havia elementos para caracterizar a suspeita de flagrante delito no interior daquele domicílio, autorizando, assim, o ingresso forçado, independentemente de autorização judicial.[76]

Como visto, o excerto em questão trata das condições para a legalidade da busca domiciliar realizada sem mandado judicial. Segundo o entendimento exposto, tal busca só é válida caso haja provas anteriores que justifiquem a necessidade da ação. Com isso, fora das excepcionalíssimas hipóteses de desnecessidade de mandado judicial, a decisão judicial que autoriza a busca deve ser fundamentada de maneira clara, destacando as razões que a tornaram necessária.

Além disso, a entrada forçada em domicílio sem mandado judicial apenas é permitida em situações de flagrante delito, e as razões que justificam essa entrada devem ser submetidas a posterior controle de legalidade pelo Poder Judiciário sob pena de, além da nulidade, haver punição civil, administrativa e criminal do agente envolvido.

Ainda sobre a inviolabilidade domiciliar, insta salientar que o Superior Tribunal de Justiça instaurou o Tema Repetitivo 1163, cuja redação foi retirada diretamente do site oficial da Corte Cidadã. A questão submetida a julgamento é a seguinte:

> Saber se a simples fuga do réu para dentro da residência ao avistar os agentes estatais e/ou a mera existência de denúncia anônima acerca da possível prática de delito no interior do domicílio, desacompanhada de outros elementos preliminares indicativos de crime, constituem ou não, por si sós, fundadas razões (justa causa) a autorizar o ingresso dos policiais em seu domicílio, sem prévia autorização judicial e sem o consentimento válido do morador.[77]

Além do mais, também se discute a legalidade de, durante a busca pessoal, a colheita de dados do aparelho eletrônico ser efetivada imediatamente pelos agentes policiais, isto é, à míngua de autorização judicial. Sobre a temática, leciona Gianluca Martins Smanio:

> [...] a comunicação em fluxo e a comunicação armazenada, junto com seus metadados intrínsecos, não podem ser objeto de busca e apreensão,

[76] MOREIRA, Leandro Mara. **Busca domiciliar: legislação, jurisprudência antidogmática e ativismo judicial**. Revista Processus de Estudos de Gestão, Jurídicos e Financeiros,Ano 15, Vol. XV, n.48, jan.-jul., 2024. P. 3. Disponível em: https://doi.org/10.5281/zenodo.10815702 Acesso em 06.10.2024

[77] STJ. Precedentes Qualificados. Disponível em: https://processo.stj.jus.br/repetitivos/temas_repetitivos/pesquisa.jsp?novaConsulta=true&tipo_pesquisa=T&sg_classe=REsp&num_processo_classe=1990972

> por estarem resguardados pelo sigilo das comunicações, nos termos do art. 5º, XII, da Constituição Federal. Desta forma, restam apenas os arquivos, dados e informações armazenados que não estão coligados à comunicação realizada entre pessoas.
> Isso gerará algumas situações: busca domiciliar, quando é encontrada máquina ou aparelho móvel contendo dados e arquivos digitais; busca pessoal, na qual é encontrada em posse do averiguado *smartphone* ou *tablet* contendo arquivos, dados e comunicações armazenadas; apreensão de informações sob a guarda de provedores de serviços de internet, como servidores de *webmail* e outros; e, por fim, a busca e apreensão por acesso remoto à máquina do indivíduo, mediante instalação de *software* ou *malware* pelo Estado.
> Quanto ao primeiro caso, é importante notar os limites presentes na decisão judicial que autorizou a busca e apreensão, além do que está limitado no escopo do respectivo mandado. Dessa maneira, caso a autorização judicial não preveja expressamente a abrangência de busca em meios digitais nos dispositivos encontrados na busca domiciliar, delimitados, localizados, a autoridade policial não pode obtê-las. Importante notar que o computador, ou HD externo, *tablet* etc.,, desde que, posteriormente, provoque a autoridade policial para realizar perícia no meio eletrônico e, assim, acessar os dados ali presentes que tenham relação com a finalidade da investigação, nos limites da decisão autorizativa.[78]

Como visto do trecho em comento, defende o autor que a comunicação em fluxo (como ligações ou mensagens em trânsito) e as comunicações armazenadas, com seus metadados, não podem ser alvo de busca e apreensão, pois são protegidas pela garantia da privacidade prevista no artigo 5º, inciso XII, da Constituição Federal. Em contrapartida, explica que o que pode ser objeto de busca e apreensão são arquivos e dados não diretamente relacionados à comunicação entre pessoas.

Com isso, explana o autor que a fundamentação das decisões judiciais é essencial para delimitar claramente o que pode ser acessado, ressaltando que, se o mandado não incluir explicitamente a busca em dispositivos digitais encontrados durante uma busca domiciliar, a autoridade policial não pode realizar essa apreensão sem nova autorização ou perícia que se vincule à finalidade investigativa, sempre respeitando os limites da decisão autorizativa.

De modo mais abrangente, o Superior Tribunal de Justiça, no Agravo Regimental no Recurso de *Habeas Corpus* 154.529/RJ, precedente retirado da página de pesquisa do site oficial do STJ[79], passou a adotar o entendimento de que "os dados armazenados nos aparelhos celulares decorrentes de envio ou recebimento de dados via mensagens SMS,

[78] SMANIO, op. cit. p. 174.

[79] As palavras-chave utilizadas na pesquisa do julgado na página oficial do STJ: https://scon.stj.jus.br/SCON/ foram: "acesso"; "mensagens"; "Whatsapp"; "inviolabilidade"; "permissão".

programas ou aplicativos de troca de mensagens" são abarcados pelo artigo 5º, X, da Constituição da República, devendo seu acesso preceder de autorização judicial, além de que a prova da validade do consentimento do proprietário é ônus da autoridade policial:

> AGRAVO REGIMENTAL NO RECURSO ORDINÁRIO EM HABEAS CORPUS. ASSOCIAÇÃO PARA O TRÁFICO DE DROGAS. TRANCAMENTO DA AÇÃO PENAL. 1. PROVAS OBTIDAS POR MEIO DE ACESSO A MENSAGENS TROCADAS PELO WHATSAPP. INFORMAÇÕES RELACIONADAS À VIDA PRIVADA E À INTIMIDADE. INVIOLABILIDADE. ART. 5°, X, DA CARTA MAGNA. ACESSO E UTILIZAÇÃO. NECESSIDADE DE AUTORIZAÇÃO JUDICIAL. SUPOSTA PERMISSÃO DO ACUSADO. AUSÊNCIA DE ELEMENTOS QUE CORROBORAM A VERSÃO DOS POLICIAIS. 2. VÍNCULO ASSOCIATIVO. AUSÊNCIA DE INDÍCIOS DE ESTABILIDADE E PERMANÊNCIA. AGRAVO REGIMENTAL NÃO PROVIDO. 1. O exame do aparelho celular do paciente durante o flagrante constitui situação não albergada pelo comando do art. 5º, inciso XII, da Constituição Federal, o qual assegura a inviolabilidade das comunicações, por outro lado, os dados armazenados nos aparelhos celulares decorrentes de envio ou recebimento de dados via mensagens SMS, programas ou aplicativos de troca de mensagens (dentre eles o "WhatsApp"), estão relacionados com a intimidade e a vida privada do indivíduo, o que os torna invioláveis, nos termos do art. 5°, X, da Carta de 1988. 2. A acusação assevera que o acesso ao telefone celular teria sido autorizado pelo próprio acusado. A situação permite a aplicação, por analogia, do entendimento jurisprudencial que está sendo construído nesta Corte Superior acerca do ingresso de policiais no interior de residências nas hipóteses de crime permanente. Sobre esse tema, o Superior Tribunal de Justiça tem exigido, em caso de dúvida, prova da legalidade e da voluntariedade do consentimento, a ser feita, sempre que possível, com testemunhas e com registro da operação por meio de recursos audiovisuais. 3. Nesse caso, o contexto narrado não traz indicações de que a permissão teria ocorrido livre de constrangimento ou coação, considerando, ainda, a clara situação desfavorável do agravado, abordado por guarnição da Polícia Militar, trazendo dúvidas quanto à voluntariedade do consentimento, que devem ser dirimidas em favor do acusado. 4. O crime de associação para o tráfico de drogas exige demonstração de animus de associar-se de modo estável e permanente, com o fito de cometer os crimes descritos na Lei n. 11.343/2006. *In casu*, não é possível constatar indícios apontando a participação do acusado no grupo criminoso, sobretudo quando se excluem os elementos obtidos de maneira ilícita, como mencionado linhas acima. 5. Agravo regimental não provido. (AgRg no RHC n. 154.529/RJ, relator Ministro Reynaldo Soares da Fonseca, Quinta Turma, julgado em 19/10/2021, DJe de 25/10/2021.)

Como exposto, restou definido que o acesso às mensagens do *WhatsApp* durante um flagrante, embora não esteja protegido pela inviolabilidade das comunicações (artigo 5º, XII, da CRFB), são abarcados pelo direito fundamental à intimidade e à vida privada (artigo 5º, X, da CRFB), sendo necessária autorização judicial para que a autoridade

policial possa acessar e utilizar dados dos dispositivos eletrônicos, a menos que haja consentimento voluntário e legal, cujo ônus de comprovação do consentimento do proprietário é do Estado.

A legalidade da coleta de dados, dessarte, está intrinsecamente ligada à observância dos direitos do investigado, incluindo o direito à privacidade (artigo 5º, X, da CRFB). Com isso, ainda cabe destacar que o acórdão mencionado foi proferido antes da entrada em vigor da Emenda Constitucional 115 de 2022, a qual, conforme supramencionado, incluiu como direito fundamental "o direito à proteção dos dados pessoais, inclusive nos meios digitais.".

Assim, embora nas situações de flagrante a polícia possa realizar a busca e apreensão sem a necessidade de autorização judicial - desde que a ação seja imediata e necessária para a captura do autor do crime ou para a preservação de provas -, a atuação policial deve respeitar os limites legais e constitucionais, evitando abusos de poder e garantindo que a coleta de provas seja realizada dentro dos limites do princípio da legalidade.

Não obstante, restou demonstrado que o Superior Tribunal de Justiça afirma que o ônus da prova recai sobre o Estado no tocante à demonstração da legalidade e voluntariedade do consentimento para a limitação das garantias individuais[80].

Especificamente no que se refere ao acesso aos dados armazenados em nuvem, Gianluca Martins Svanio explica que, a partir da entrada em vigor do Marco Civil da Internet, o mandado de busca e apreensão deve ser específico para autorizar o acesso aos dados nos endereços dos servidores externos, não podendo, de forma alguma, o mandado conter comandos genéricos:

> Situação diametralmente oposta encontra-se nos dados e arquivos armazenados em servidores externos à máquina do indivíduo, como acessados remotamente. Como o mandado de busca e apreensão possui localização exata da medida restritiva a ser realizada, não pode conter descrições genéricas. Dessa maneira, apenas e tão somente os dados e

[80] "Enquanto não se atinge esse patamar ideal, diante da possibilidade de que se criem discursos ou narrativas dos fatos para legitimar a diligência policial, deve-se, no mínimo, exigir que se exerça um "especial escrutínio" sobre o depoimento policial, na linha do que propôs o Ministro Gilmar Mendes por ocasião do julgamento do Tema de Repercussão Geral n. 280: "O policial pode invocar o próprio testemunho para justificar a medida. Claro que o ingresso forçado baseado em fatos presenciados pelo próprio policial que realiza a busca coloca o agente público em uma posição de grande poder e, por isso mesmo, deve merecer especial escrutínio". BRASIL, Superior Tribunal de Justiça (6ª Turma). ***Habeas Corpus* 831416 - RS (2023/0205387-0)**. Relator Ministro Rogerio Schietti Cruz, julgado em 20.8.2024, DJe de 29.8.2024. Disponível em: https://scon.stj.jus.br/SCON/. Palavras-chave para pesquisa: "dropsy testimony".

> arquivos presentes naquele endereço podem ser alvo de busca e apreensão. Isso não quer dizer que tais dados não possam ser acessados pelos agentes policiais, desde que haja ordem judicial específica para o endereço da localidade dos servidores externos, ou que o acesso remoto esteja abrangido por decisão judicial, com especificidade quanto ao procedimento. Com o Marco Civil da Internet, a responsabilidade do provedor de serviços e aplicações de Internet foi positivada, exigindo deveres de proteção à intimidade e privacidade do detentor desses dados. Por estarmos diante de direitos fundamentais, a lei exige autorização judicial para que os agentes solicitem dados e arquivos pessoais do usuário a esses provedores, que, respeitando os ditames legais e os princípios constitucionais, mediante ordem judicial, podem entregá-los às autoridades para fins de investigação.[81]

Nos termos do trecho em comento, quando se trata de busca e apreensão, o mandado precisa especificar o local exato onde será executado, sem descrições vagas, pois apenas os dados e arquivos no local mencionado podem ser apreendidos, sob pena de pescaria probatória.

Assim, apenas caso houver ordem judicial que especifique o endereço dos servidores externos ou autorize o acesso remoto, os dados poderão ser obtidos legalmente. Isso, pois o Marco Civil da Internet reforça a responsabilidade dos provedores de serviços em proteger a privacidade dos usuários, garantindo que o processo siga os princípios constitucionais.

No tocante à posição firmada na jurisprudência quanto ao acesso aos dados armazenados em nuvem, compreende o Superior Tribunal de Justiça que a tal modalidade de armazenamento, amplamente adotado por empresas nacionais e internacionais, permite que dados sejam guardados em servidores espalhados pelo mundo.

No entanto, essa flexibilidade de armazenar dados globalmente não isenta as empresas da responsabilidade de fornecer essas informações às autoridades judiciais brasileiras quando há uma investigação criminal relacionada a crimes cometidos no Brasil. Dessarte, ainda que os dados estejam localizados fora do território nacional, as empresas que operam no Brasil ainda devem cumprir a legislação brasileira e colaborar com a justiça caso instadas a prestar informações ao Juízo[82].

---

[81] SMANIO, op. cit. p. 175.

[82] "Acrescento que o armazenamento em nuvem, estrategicamente utilizado por diversas empresas nacionais e estrangeiras, possibilita que armazenem dados em todos os cantos do globo, sem que essa faculdade ou estratégia empresarial possa interferir na obrigação de entregá-los às autoridades judiciais brasileiras quando envolvam a prática de crime em território nacional." *In*: **RMS n. 66.392/RS**, relator Ministro João Otávio de Noronha, Quinta Turma, julgado em 16/8/2022, DJe de 19/8/2022. Disponível em: https://scon.stj.jus.br/SCON/ Palavras-chave para busca: "quebra" "sigilo" "dados" "nuvem".

Após a extração de dados, também é imprescindível que se tome cuidado com sua gestão. Nos termos do artigo 158-A do Código de Processo Penal, a manutenção da rigidez da cadeia de custódia da prova coletada, com a finalidade de manter a integridade dos dados, é importante para evitar seu perdimento ou modificação:

> Apreendido o dispositivo mediante ordem judicial, a atividade pericial exige cuidados relativos à *cadeia de custódia* da prova, assim compreendido "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" (art. 158-A do CPP).
> Um método valioso para a sua preservação consiste no uso de ferramentas de *hashing*. Cuida-se de operação realizada por meio de aplicativo que cria um código único (*hash*) para quaisquer dados que sejam nele inseridos, tornando-se extremamente relevante para fins de preservação da integridade de uma evidência digital coletada. A título de exemplo, ao se utilizar o aplicativo de *hashing* no conteúdo de um disco rígido (HD) externo ou no conteúdo armazenado por um aparelho celular, será gerado um número *hash* único. Se um único arquivo daquela base de dados for modificado, o número *hash* será diverso. Assim, qualquer alteração no conteúdo poderá ser identificada pela comparação entre número *hash* inicial e o número após a suposta alteração, tornando-se inservível a prova.[83]

O autor explica que, após a apreensão de um dispositivo a partir de uma ordem judicial, é crucial seguir a cadeia de custódia da prova, a qual se dá com a documentação do percurso da evidência desde sua coleta até o descarte, garantindo sua integridade e autenticidade.

A título de exemplo, uma ferramenta fundamental para essa preservação é o uso do *hashing*, que gera um código único (*hash*) para os dados inseridos. Esse código serve como uma "impressão digital" da evidência digital, de modo que, se qualquer alteração for feita no conteúdo, o *hash* resultante será diferente do original, o que permite identificar eventuais modificações, garantindo que a prova digital se mantenha intacta e confiável para a investigação.

No julgamento do Agravo Regimental no *Habeas Corpus* 828.054/RN[84], o Superior Tribunal de Justiça, ao dar provimento ao recurso para reconhecer a

[83] LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. 2.ed., rev. e atual. 2 São Paulo: Editora JusPodivm. 2024. P. 326.

[84] "A observação do princípio da mesmidade visa a assegurar a confiabilidade da prova, a fim de que seja possível se verificar a correspondência entre aquilo que foi colhido e o que resultou de todo o processo de extração da prova de seu substrato digital. Uma forma de se garantir a mesmidade dos elementos digitais é a utilização da técnica de algoritmo hash, a qual deve vir acompanhada da utilização de um software confiável, auditável e amplamente certificado, que possibilite o acesso, a interpretação e a extração dos

inadmissibilidade das provas, enfatizou que a cadeia de custódia é fundamental para garantir a integridade das provas digitais, desde sua coleta até a análise judicial.

No contexto de provas extraídas de dispositivos como celulares, a Corte ressaltou que a volatilidade e facilidade de alteração dos dados exigem cuidados rigorosos, sendo uma das técnicas indicadas o uso de algoritmos de *hash*, que geram um código único para os dados coletados, assegurando que qualquer modificação seja detectada, garantindo a correspondência entre a prova original e sua versão apresentada no processo, preservando a confiança e a integridade do material:

> Em relação a identificação de mídias, o processo diz respeito tanto à identificação física quanto a identificação lógica que é realizada através do cálculo do valor (ou código) hash, utilizando funções como MD5 (Memory Digest Algorithm - Resumo da memória), SHA1 (Secure Hash Algorithm Algoritmo de hash seguro) ou SHA2 - mais utilizada atualmente. Em relação à preservação da prov a digital, a norma diz respeito à proteção de sua integridade para garantia de sua utilidade e validade probatória. O processo de preservação envolve a guarda da evidência digital e do dispositivo digital visando garantir a autenticidade da evidência digital. Deve ser minimizado o manuseio da evidencia e dispositivo informático. Todas as alterações e ações devem ser documentadas. Salienta-se, ainda, que o perito forense deve praticar ações somente dentro de sua área de competência.[85]

Conforme exposto, a identificação de mídias no processo penal abrange dois aspectos: a identificação física dos dispositivos de armazenamento - os quais podem ser apreendidos quando do cumprimento de mandado de busca e apreensão - e a identificação lógica, que é feita por meio de códigos *hash.*

Esses códigos, gerados por algoritmos como MD5, SHA1 ou SHA2, servem para calcular uma "impressão digital" única da mídia. O *hash* é crucial para garantir a integridade da prova digital, pois qualquer alteração no conteúdo da mídia resultaria em um código *hash* diferente, invalidando a prova.

Assim, a preservação da prova digital se concentra em proteger sua integridade, garantindo que ela permaneça autêntica e inalterada até ser analisada, porquanto todo processo de coleta e análise precisa ser documentado, apenas profissionais qualificados

---

dados do arquivo digital." **AgRg no HC n. 828.054/RN**, relator Ministro Joel Ilan Paciornik, Quinta Turma, julgado em 23.4.2024, DJe de 29.4.2024. Disponível em: https://scon.stj.jus.br/SCON/. Palavra-chave: "*hash*".

[85] 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. ISSN 1984-7858. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130. P. 10. Acesso em 26.08.2024

(peritos) detém autorização de realizar essas ações, garantindo que a documentação rigorosa e o uso de *hashes* preservem a evidência e mantenha sua validade probatória em juízo.

Em suma, a discussão em torno da legalidade da coleta e gestão de dados em aparelhos eletrônicos durante as investigações é um reflexo das complexidades do mundo digital contemporâneo, tendo a jurisprudência avançado no sentido de garantir que a privacidade dos indivíduos seja respeitada, mesmo em situações de investigação criminal.

Assim, a construção de um arcabouço jurídico que respeite os direitos fundamentais, ao mesmo tempo em que permite a efetividade das ações policiais, é essencial para a manutenção do Estado de Direito e para a promoção de uma justiça que encontre um equilíbrio entre a eficiência e o respeito aos direitos fundamentais dos réus e investigados.

2.3. A Lei n. 12.965/2014 e a jurisprudência brasileira sobre o acesso de dados armazenados em nuvem

Dentro do campo infraconstitucional, as disposições do artigo 3º, II, III, artigo 7º, I, II, III, VII e artigos 10 e 11 da Lei 12.965/2014 (Marco Civil da internet) asseguram várias proteções à privacidade, aos dados pessoais, à vida privada, ao fluxo de comunicações e às comunicações privadas dos usuários da internet. Conforme preceitua a própria descrição da Lei, esta é responsável por estabelecer "princípios, garantias, direitos e deveres para o uso da internet no Brasil"[86], abrangendo aspectos como a proteção da privacidade, a neutralidade da rede e a liberdade de expressão.

Acerca do objetivo do Marco Civil da Internet, vale mencionar a seguinte lição doutrinária de Victor Sales Pinheiro e Alexandre Pereira Bonna:

> As mudanças que essa revolução tecnológica causa são tão radicais e imediatas que dificilmente o Direito consegue compreendê-las e acompanhá-las. Antes da promulgação da Lei 12.965/2014, havia grande insegurança jurídica sobre o direito do mundo eletrônico, com o extensivo apelo a princípios constitucionais, analogias, doutrinas e jurisprudência, muitas vezes desconexos entre si.
> No ordenamento jurídico nacional, a primeira normatização sistemática do ciberespaço se deu com essa lei, chamada Marco Civil da Internet, pautado na vocação constitucional de proteger os direitos fundamentais

[86] BRASIL. **Marco Civil da Internet (2014)**. Lei 12.965 de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

> do nosso Estado de Direito, sobretudo o direito à privacidade, tão vulnerável na rede mundial de computadores, seja pela sua invasão privada - como pela divulgação de dados cadastrais com fins comerciais e políticos -, seja pela intromissão pelo próprio Estado - como em sede de investigação policial ou judicial.[87]

O trecho em apreço destaca que a revolução tecnológica trouxe mudanças tão rápidas e profundas que o Direito atual possui dificuldade em compreendê-las e se adaptar a elas[88]. É mencionado que, antes da Lei 12.965/14, havia considerável insegurança jurídica em relação ao direito no ambiente digital devido ao uso disperso de princípios constitucionais, analogias, doutrinas e jurisprudência que muitas vezes não se conectavam adequadamente.

O Marco Civil da Internet representou a primeira tentativa de regulamentar o ciberespaço de forma sistemática, com o objetivo principal de proteger os direitos fundamentais, especialmente o direito à privacidade, que está altamente vulnerável na internet, principalmente por invasões privadas, como o risco de divulgação de dados pessoais com fins comerciais ou políticos, e por intervenções do próprio Estado, como em investigações policiais ou judiciais *lato sensu*.

Nesse cenário jurídico, o artigo 7º, III, dessa Lei é claro ao estabelecer a inviolabilidade e o sigilo das comunicações privadas armazenadas (dados armazenados), excetuando a hipótese da "ordem judicial":

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;[89]

Dessa forma, o debate gira em torno de saber se as decisões judiciais que determinam a quebra de sigilo telemático para o acesso aos dados digitais estáticos devem ser fundamentadas com os mesmos requisitos exigidos para as decisões que autorizam as interceptações telefônicas.

---

[87] PINHEIRO, Victor Sales; BONNA, Alexandre Pereira. **Sociedade da informação e direito à privacidade no Marco Civil da Internet: fundamentação filosófica do Estado de Direito**. Revista de Direitos e Garantias Fundamentais, *[S. l.]*, v. 21, n. 3, p. 365–394, 2020. P. 366. DOI: 10.18759/rdgf.v21i3.1555. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1555. Acesso em 20.08.2024

[88] Ibidem, p. 367.

[89] BRASIL. **Marco Civil da Internet**. Lei Federal 12.965/14, de 23.04.2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Assim, apesar de prever uma exceção ao direito à privacidade dos dados, o Marco Civil não estipulou nenhum *standard* de fundamentação das decisões judiciais proferidas com a finalidade de autorizar o acesso aos dados armazenados, tendo se limitado a relativizar esse direito a partir de simples comando abstrato que não vincula o Juízo a se valer de um padrão mínimo em expor sua *ratio decidendi*:

Por outro lado, a Lei 9.296/96, responsável por regular a interceptação de comunicações telefônicas e de dados, permitindo a coleta de provas em investigações criminais, fixou em seu artigo 2º diversos requisitos para que uma decisão judicial seja considerada minimamente fundamentada:

> Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
> I - não houver indícios razoáveis da autoria ou participação em infração penal;
> II - a prova puder ser feita por outros meios disponíveis;
> III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.
> Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.[90]

Tal dispositivo determina que a interceptação só é permitida em situações específicas, as quais incluem indícios razoáveis, de modo que a interceptação só pode ocorrer se houver indícios suficientes que sugiram que a pessoa está envolvida em um crime; se a prova do crime puder ser obtida por outros meios que não a interceptação, essa alternativa deve ser utilizada, devendo ser priorizados os métodos que não invadam a privacidade; e, finalmente, a natureza do crime, não sendo a interceptação permitida para apurar crimes punidos apenas com detenção.

Diferentemente do Marco Civil da Internet, para as interceptações telefônicas o legislador demonstrou preocupação em não violar a privacidade em casos que não envolvem crimes graves. Além disso, o parágrafo único do artigo 2º da Lei 9.296/96 enfatiza que, em qualquer situação, a investigação deve ser claramente justificada, com a descrição do que está sendo investigado e a identificação dos envolvidos, a menos que isso seja impossível de ser feito.

[90] BRASIL. **Lei de Interceptação Telefônica**. Lei Federal 9.296/96, de 24.07.1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm

Devido a essa diferenciação, a principal problemática apresentada reside no fato de que a jurisprudência, em razão do princípio da especialidade das normas, vem adotando graus de fundamentação distintos para as interceptações telefônicas - realizadas em tempo real, sendo aplicável a Lei 9.296/96 - e para o acesso aos dados já armazenados os Tribunais aplicam a Lei 12.965/14, cujo grau de fundamentação exigível é menor.

Acerca do princípio da especialidade das normas, assim ensina o professor Cezar Roberto Bittencourt:

> Considera-se especial uma norma penal, em relação a outra geral, quando reúne todos os elementos desta, acrescidos de mais alguns, denominados especializantes. Isto é, a norma especial acrescenta elemento próprio à descrição típica prevista na norma geral. Assim, como afirma Jescheck , "toda a ação que realiza o tipo do delito especial realiza também necessariamente, ao mesmo tempo, o tipo do geral, enquanto o inverso não é verdadeiro". A regulamentação especial tem a finalidade, precisamente, de excluir a lei geral e, por isso, deve precedê-la (*lex specialis derogat lex generalis*).[91]

Nesse contexto, justamente em razão da diferença entre o instituto da interceptação telefônica e da proteção aos dados já armazenados, seja em aparelhos telefônicos ou na memória de algum computador, *pendrive* ou *nuvem*, o padrão de fundamentação exigido para a decretação de um ou de outro muda consideravelmente.

É o que se pode constatar da atual orientação da jurisprudência do Superior Tribunal de Justiça, que caminha no sentido de conferir diferentes proteções ou *standards* probatórios para a decretação de acesso aos dados estáticos e para a interceptação - instantânea - de dados em movimento:

> AGRAVO REGIMENTAL NO RECURSO ORDINÁRIO EM HABEAS CORPUS. QUEBRA DE SIGILO TELEMÁTICO. NULIDADE. AUSÊNCIA. LEI N. 12.965/2014. NORMA MAIS ESPECÍFICA. DADOS ESTÁTICOS. DECISÕES DEVIDAMENTE FUNDAMENTADAS. OBTENÇÃO DE RIF. COMPARTILHAMENTO DIRETO ENTRE O COAF E MINISTÉRIO PUBLICO. TEMA 990. BUSCA ESPECULATIVA. NÃO EVIDENCIADA. AGRAVO REGIMENTAL DESPROVIDO.
> 1. Inaplicabilidade das disposições da Lei n. 9.296/1996, pois a Lei n. 12.965/2014, por ser mais específica, incide em detrimento daquela à presente hipótese, que diz respeito a dados estáticos, ou seja, a conversas já armazenadas nas contas de e-mail, e não acesso em tempo real. Não havendo interceptação, mas acesso a informações armazenadas, a

[91] BITTENCOURT, Cezar Roberto. **Tratado de Direito Penal: Parte Geral (arts. 1º a 120)**. 29. ed. – São Paulo: SaraivaJur, 2023. (v. 1) . P. 213-214.

> quebra de sigilo aqui determinada não está abrangida pela lei que disciplina a inviolabilidade das comunicações telefônicas (Lei n. 9.296/1996), incidindo à hipótese a Lei do Marco Civil (Lei n. 12.965/2014), que assegura a inviolabilidade de conversas particulares e o sigilo de comunicações privadas armazenadas, exceto por ordem judicial. 2. Decisões que deferiram a quebra do sigilo de conteúdos de comunicação armazenados em contas de e-mails que contêm suficiente fundamentação, diante dos fundados indícios de ocorrência de ilícitos - fraudes em licitação, peculato, corrupção, formação de cartel e organização criminosa supostamente praticados por Servidores Públicos da Prefeitura Municipal de Orlândia - SP em conluio com alguns empresariados locais -, com descrição individualizada da suposta conduta criminosa de cada um dos envolvidos. 3. Aplicabilidade ao caso das diretrizes estabelecidas pelo Supremo Tribunal Federal no julgamento do Terma 990 de sua repercussão geral no que toca à obtenção de RIF sem prévia autorização judicial, mediante compartilhamento direto entre COAF e autoridades atuantes em persecução penal. 4. Ausência de demonstração, no caso, da nefasta prática denominada de pesca predatória (fishing expedition), na medida em que não evidenciada a busca especulativa por provas a serem produzidas em face dos investigados. 5. Agravo regimental desprovido. (AgRg no RHC n. 189.011/SP, relator Ministro Ribeiro Dantas, Quinta Turma, julgado em 18/3/2024, DJe de 21/3/2024.)[92]

Como observado, o precedente analisado destaca uma importante diferenciação na fundamentação exigível para a interceptação telefônica/telemática e para o acesso a dados armazenados. Segundo o acórdão, nas interceptações telefônicas ou telemáticas, regidas pela Lei 9.296/96, esta é aplicável em casos de comunicações em tempo real.

Por sua vez, a Lei 12.965/14 (Marco Civil da Internet), que é reputada como mais específica para a quebra do sigilo de arquivos armazenados, é aplicável aos casos envolvendo o acesso a dados estáticos, podendo ser citadas como exemplo as listas de contatos, galeria de imagens, conversas de *WhatsApp*, e-mails, bloco de notas, histórico da frequência dos batimentos cardíacos, dentre outros inúmeros aplicativos com potencial para armazenar informações sensíveis ou não.

Como consequência disso, a questão da proteção dos dados estáticos em comparação com as interceptações telefônicas é um tema que merece uma análise crítica aprofundada. Embora o Marco Civil da Internet tenha sido um avanço significativo na regulamentação do ciberespaço[93], a disparidade na proteção conferida aos dados estáticos

[92] STJ. Disponível em: https://scon.stj.jus.br/SCON/. Palavras-chave: “Dados estáticos”, “quebra”, “sigilo”, “Marco Civil”.

[93] Acerca da definição de do termo “ciberespaço” e seus contornos jurisdicionais: “Em termos práticos, o ciberespaço se concretiza territorialmente com qualidades transfronteiriças de operação e circulação de dados. Assim, um simples e-mail enviado do Brasil para a Índia por meio de uma conta da empresa estadunidense Microsoft (Hotmail), cuja central de dados está na Irlanda, envolve no mínimo quatro

e às comunicações em andamento levanta preocupações sobre a integridade do direito à privacidade no Brasil.

Primeiramente, é importante destacar que o artigo 7º, III, do Marco Civil da Internet assegura a inviolabilidade e o sigilo das comunicações privadas armazenadas, mas não estabelece um padrão rigoroso de fundamentação para as decisões judiciais que autorizam a quebra desse sigilo. Isso, por sua vez, contrasta com a Lei 9.296/96, que regula as interceptações telefônicas e exige uma fundamentação robusta e específica para a autorização de tais medidas.

Por conseguinte, a falta de um padrão mínimo de fundamentação para a quebra de sigilo telemático pode resultar em decisões judiciais arbitrárias e desproporcionais, sobretudo tendo em vista que computadores e celulares armazenam muito mais informações sensíveis do que o conteúdo de rápidas trocas de informação por meio verbal em um curto lapso de tempo:

> No cenário contemporâneo a forma muito comum de conexão entre as pessoas é no meio digital. Nele, se transmite sentimentos, imagens, momentos e promove a aproximação de pessoas que não estão fisicamente pertos. Mas conforme a internet evoluía, passou-se a realizar diversas atividades online. Compras na Amazon, leitura de ebooks, revistas científicas online, jornalismo digital, conexões internacionais, e, claro, serviços de streaming e redes sociais. Neste cenário algo comum na maioria dos sites que os usuários acessam, tanto para fazer compras quanto para navegar pelas redes sociais, são os termos e condições de uso.
>
> Nestes termos, sob o argumento do consentimento, as empresas passam a monitorar todos os rastros digitais dos usuários, violando a privacidade e até mesmo utilizando os dados coletados para fins antidemocráticos. Estes dados coletados, inclusive os fornecidos livremente pelo usuário ao concordar com os termos, geram composições, juntamente com dados armazenados online que acabam vazados. Existem também os dados extraídos das transações que o usuário efetuou pela internet, e, num contexto mais abrangente, inclusive as câmeras de vigilância, ligações telefônicas, extratos bancários e prontuários médicos.[94]

jurisdições diferentes. Ou seja, a Internet cria atividades, atores e espaços transfronteiriços que não se sobrepõem ponto a ponto ao território westfaliano tradicional, mas que tecem uma rede de relações através de uma rede de objetos.". ISRAEL, Carolina Batista. **Território, jurisdição e ciberespaço: entre os contornos westfalianos e a qualidade transfronteiriça da Internet**. Geousp – Espaço e Tempo (On-line), v. 24, n. 1, p. 69-82, abr. 2020. ISSN 2179-0892. P. 73. Disponível em: https://doi.org/10.11606/issn.2179-0892.geousp.2020.161521 Acesso em 03.08.2024

[94] BENDLIN, Rafaela Witt.; WITT, Cleonice. **A interseção entre proteção de dados e direito à privacidade no contexto digital**. CONTRIBUCIONES A LAS CIENCIAS SOCIALES, [S. l.], v. 17, n. 7, p. e8250, 2024. DOI: 10.55905/revconv.17n.7-112. P. 1 e 2. Disponível em: https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/8250 Acesso em 06.11.2024

Diante do perigo constatado por toda exposição digital, a decisão que decreta a quebra dos dados estáticos, que muitas vezes contêm informações sensíveis e pessoais, deveria seguir os mesmos requisitos de fundamentação que as decisões que determinam interceptações telefônicas, pois a ausência de requisitos rigorosos se mostra desproporcional, podendo levar a abusos e violações da privacidade dos cidadãos.

Nesse aspecto, como demonstrado anteriormente, a jurisprudência brasileira tem adotado uma abordagem que parece desconsiderar a vulnerabilidade dos cidadãos ante ao conteúdo dados estáticos. Esses dados, que podem incluir informações sobre a vida pessoal, financeira e profissional dos indivíduos, merecem proteção equivalente àquela conferida às comunicações em tempo real, pois não há sentido teleológico em conferir menos proteção a informações muito mais sensíveis do que as passíveis de serem captadas em interceptações telefônicas ou telemáticas.

Isso, pois a falta de fundamentação adequada pode resultar em um tratamento desigual, desproporcional e, consequentemente, injusto. Nessa esteira, a necessidade de um padrão de fundamentação mais rigoroso é ainda mais evidente quando se considera o potencial de uso indevido das informações obtidas por meio da quebra de sigilo, porquanto inexiste previsão legislativa específica sobre a cadeia de custódia para regular a gestão de dados coletados em investigações criminais, tratando-se de trabalho árduo que vem sendo realizado pela jurisprudência.

A título de exemplo, vale mencionar o Agravo Regimental no Habeas Corpus 828054-RN, julgado pela 5ª Turma do Superior Tribunal de Justiça no dia 23.04.2024. Naquela oportunidade, foi destacado o princípio da mesmidade, o qual tem como objetivo garantir a confiabilidade da prova digital, assegurando que o que foi coletado inicialmente corresponde exatamente ao que é extraído e analisado ao longo do processo.

Para garantir essa correspondência, o precedente em comento convalidou a aludida técnica de algoritmo *hash*, que gera um código único para cada arquivo. Para tanto, ainda destacou a Corte que, para garantir a efetividade do processo, é essencial que o *software* utilizado seja confiável, auditável e amplamente certificado, assegurando que o acesso, a extração e a interpretação dos dados sejam precisos e válidos, preservando a integridade da prova.[95]

[95] "A observação do princípio da mesmidade visa a assegurar a confiabilidade da prova, a fim de que seja possível se verificar a correspondência entre aquilo que foi colhido e o que resultou de todo o processo de extração da prova de seu substrato digital. Uma forma de se garantir a mesmidade dos elementos digitais é a utilização da técnica de algoritmo hash, a qual deve vir acompanhada da utilização de um software confiável, auditável e amplamente certificado, que possibilite o acesso, a interpretação e a extração dos

Nessa esteira, o Projeto de Lei 1515/2022, cujo objetivo é a criação de uma "LGPD Penal", embora esteja com o trâmite estagnado desde 20.06.2022, estabelece princípios interessantes para o compartilhamento de dados colhidos nas investigações criminais:

> Art. 4º As atividades de tratamento e compartilhamento de dados pessoais em matéria de segurança do Estado, de defesa nacional, de segurança pública e de persecução penal deverão observar a boa-fé e os seguintes princípios:
> I - licitude: embasamento do tratamento de dados pessoais em hipótese legal, nos termos do Capítulo II desta Lei;
> II - finalidade: coletados para fins determinados, explícitas e legítimas, e não tratados de uma forma incompatível com essas finalidades, de modo a subsidiar a atuação dos órgãos incumbidos das atividades de segurança pública, investigação e repressão de infrações penais, em conformidade com suas atribuições legais;
> III - adequação: pertinência e relevância do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento;
> IV - necessidade: limitação do tratamento ao necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> V - segurança da informação: utilização de medidas físicas, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VI - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> VII - supremacia do interesse público: prevalência do interesse público em conflito sobre um interesse particular;
> VIII - qualidade dos dados: garantia de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - auditabilidade: a tomada de medidas que viabilizem a verificação e a checagem do tratamento, bem como o controle do acesso à informação, sempre que tecnicamente possível.[96]

Os princípios descritos no artigo 4º do Projeto de Lei 1.515/2022 regulam o tratamento e compartilhamento de dados pessoais em investigações criminais, assegurando que essas atividades sejam realizadas com base na lei e com boa-fé, exigindo que o tratamento de dados seja feito de forma legal, para fins específicos e legítimos, sem desvio de finalidade.

---

dados do arquivo digital." *In*: **AgRg no HC n. 828.054/RN**, relator Ministro Joel Ilan Paciornik, Quinta Turma, julgado em 23/4/2024, DJe de 29/4/2024. Disponível em:https://scon.stj.jus.br/SCON/. Palavra-chave: *Hash*.

[96] Projeto de Lei 1515/2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274&filename=PL%201515/2022

Preceitua o dispositivo que o tratamento deve ser adequado ao contexto e limitado ao necessário, sem excessos, sendo essencial garantir a segurança da informação, prevenindo acessos não autorizados, de modo que o interesse público deve prevalecer sobre interesses particulares, e os dados devem ser precisos e atualizados para cumprir sua finalidade, evitando-se qualquer tipo de discriminação e estipulando mecanismos para auditar e controlar o acesso aos dados sempre que possível.

Considerando que o Projeto de Lei ainda não foi aprovado, sem uma justificativa adequada, necessária e proporcional às decisões que decretam o acesso aos dados estáticos, há elevado risco de que dados pessoais sensíveis sejam utilizados de maneira inadequada, comprometendo a privacidade e a segurança dos indivíduos.

Com isso, a jurisprudência deve se alinhar aos princípios constitucionais que garantem a proteção da privacidade e dos dados pessoais, exigindo para a quebra de dados estáticos os mesmos requisitos de fundamentação presentes no artigo 2º da Lei 9.296/96, que exige indícios razoáveis e a descrição clara da situação objeto da investigação.

Tal interpretação analógica garantiria que as decisões judiciais fossem fundamentadas em critérios objetivos e transparentes, justificando principalmente a insuficiência da não utilização de métodos investigativos menos invasivos. Além disso, a aplicação de requisitos rigorosos para a quebra de sigilo telemático poderia contribuir para a construção de uma cultura de respeito à privacidade no ambiente digital, hipótese essa que traria mais resultados do que o simples incremento legislativo.

Dessarte, considerando a crescente digitalização da sociedade e o aumento do volume de dados pessoais disponíveis online, notadamente em um cenário em que as informações são facilmente acessíveis, é certo afirmar que a proteção dos dados estáticos se torna ainda mais crucial, pois a proteção da privacidade não deve ser seletiva; todos os dados pessoais, independentemente de sua forma de armazenamento ou se estão em fluxo no momento da captação, merecem a mesma proteção jurídica.

Dessarte, conforme analisado, defende a jurisprudência dominante que o direito à inviolabilidade das comunicações não inclui os dados registrados, adotando uma leitura mais limitada do artigo 5º, XII, da Constituição da República, segundo o qual:

> Art. 5º, XII. é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Por conseguinte, essa interpretação do "AgRg no RHC n. 189.011/SP, relator Ministro Ribeiro Dantas" - a qual inclusive foi proferida após a inserção do inciso LXXIX no artigo 5º da Constituição Federal - caminha no sentido de que somente as comunicações telefônicas e telemáticas em andamento estão protegidas pela norma fundamental, implicando, consequentemente, na exclusão da tutela dos dados armazenados.

O inciso XII do artigo 5º da Constituição Federal, ao estabelecer a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, condicionou seu acesso à prévia decisão judicial, porém deixou de especificar qual o grau - o *standard* probatório - exigível para a que seja considerado minimamente fundamentado o decreto da quebra de sigilo de dados armazenados em nuvem ou em armazenamento na memória interna dos dispositivos eletrônicos.

Apesar disso, a regulamentação infraconstitucional dada pela Lei 9.296/96 às interceptações telefônicas prescreveu, em seu artigo 2º, II[97], como padrão de fundamentação a necessária comprovação da inexistência de outros meios disponíveis para a produção da prova, sob pena de indeferimento do pedido.

Diante disso, no julgamento do Recurso Extraordinário 418.416/SC (DJe 19/12/2006), sob a relatoria do Ministro Sepúlveda Pertence, argumentou a Corte Suprema que proteger os dados propriamente ditos com o mesmo rigor que a Lei 9.296/96 tornaria inviável qualquer investigação administrativa. Nos termos da ementa, "*A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador.*"[98].

Tal entendimento foi reafirmado no julgamento do *Habeas Corpus* 91.867/PA, no qual o Supremo Tribunal Federal destacou a distinção entre a comunicação telefônica e os registros telefônicos, afirmando que cada um ostenta proteção jurídica específica, estando tão somente as comunicações em andamento abarcadas pela Lei 9.296/96, cujo rigor da fundamentação judicial é mais exigente, ao passo que os registros telefônicos já armazenados prescindiriam de decisão judicial para o acesso por parte dos agentes da polícia judiciária.

[97] Lei 9.296/96 - Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses: II - a prova puder ser feita por outros meios disponíveis;

[98] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 418.416/SC**. Rel. Ministro Sepúlveda Pertence. Tribunal Pleno, Brasília/DF, DJ 19.12.2006.

O referido precedente se tratava de *habeas corpus* impetrado com a finalidade de trancar por inépcia a denúncia então oferecida. Naqueles autos, foi suscitada a ilicitude das provas obtidas após a prisão em flagrante do corréu, pois os policiais, sem autorização judicial, examinaram os registros de chamadas recentes dos dois celulares apreendidos, e tais dados telemáticos foram utilizados como fundamento para o desenrolar das investigações e futuro oferecimento da denúncia.

Ao apreciar a questão, alegou o Supremo Tribunal Federal que:

> Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados.[99]

Como visto, o trecho destaca uma importante diferença entre comunicação telefônica e registros telefônicos, enfatizando que ambos possuem proteções jurídicas distintas. Em um primeiro plano, a comunicação telefônica se refere ao conteúdo das conversas entre indivíduos no momento do ato, sendo este lapso temporal protegido pela Constituição.

Em contraste, os registros telefônicos[100] são dados que documentam essas comunicações, como horários, durações e números discados, tratando-se de informações armazenadas. Além disso, o conceito de dados estáticos também inclui o registro de fotografias, vídeos, mensagens de aplicativos, informações pessoais sobre saúde, viagens, comunidades, histórico de pesquisa, dentre outros dados muito mais sensíveis e que podem estar presentes nos aparelhos telefônicos.

Esses registros, embora muitas vezes mais relevantes do que o conteúdo captado das interceptações telefônicas em andamento, sob a perspectiva adotada pelo *Habeas Corpus* 91.867/PA, não recebem pela jurisprudência dos Tribunais Superiores a mesma proteção constitucional destinada à comunicação direta entre pessoas.

---

[99] BRASIL. Supremo Tribunal Federal. **Habeas Corpus 91.867/PA**. Rel. Ministro Gilmar Mendes. 2ª Turma, Brasília/DF, DJe 20/09/2012.

[100] "A análise desses dados é bastante reveladora. Registros telefônicos são capazes de informar contatos e intensidade desses contatos; registros de uso da Internet revelam informações sobre a navegação do usuário e, assim, seus hábitos e interesses; registros de localização, decorrentes dos dados sobre a torre de rádio, informam, como já se supõe pelo nome, por onde a pessoa esteve.". ABREU, Jacqueline de Souza. **Guarda obrigatória de registros de telecomunicações no Brasil: Sobre as origens da retenção de dados e as perspectivas para direitos fundamentais**. P. 2. *In*: Disponível em: https://lavits.org/wp-content/uploads/2017/08/P5_De_Souza_Abreu.pdf

Além disso, o trecho do HC 91.867/PA esclarece que o artigo 5º, XII, da Constituição Federal protege a comunicação de dados, e não os dados armazenados. Isso significa que a inviolabilidade garantida é aplicada à troca de informações entre os usuários, garantindo a privacidade das mensagens e chamadas apenas enquanto perdurar o ato. Por sua vez, os dados armazenados, como os registros de chamadas, não são considerados cobertos pelo texto constitucional, apontando uma distinção crucial entre o conteúdo instantâneo da comunicação e os metadados que a documentam.

Atualmente, sob a perspectiva do anteriormente explicado fenômeno da mutação constitucional, a jurisprudência caminha no sentido de reconhecer, como direito fundamental, a proteção dos dados já registrados, o que pode se dar tanto pelo artigo 5º, XII, da Constituição da República, quanto pelos seu inciso X, que tutela as garantias da intimidade e da vida privada.

Nesse contexto, ainda que se considere que os dados armazenados não estejam protegidos pela norma prevista no inciso XII do artigo 5º da Constituição Federal, tais dados são abarcados pela garantia de intimidade e privacidade do inciso X do mesmo artigo. Além disso, cumpre novamente ressaltar a proteção constitucional conferida pelo novo inciso LXXIX do artigo 5º da Constituição da República.

Ademais, a Lei 12.965/2014 (Marco Civil da Internet) e outras normas infraconstitucionais avançaram para proteger esses dados, os quais apenas podem ser acessados mediante decisão judicial fundamentada a partir da adequação, necessidade e proporcionalidade em sentido estrito, garantindo um grau mínimo, porém ainda não satisfatório, de fundamentação, pois não é equiparável à proteção prevista pela Lei 9.296/96.

Ao considerar esses fatores, o Ministro Gilmar Mendes retificou seu entendimento ao alterar seu voto no julgamento do Tema 977-STF, referente ao Agravo em Recurso Extraordinário 1.042.075/RJ:

> Da mesma forma, não se mostra viável conferir acesso parcial às informações contidas nos aparelhos celulares, uma vez que tal posicionamento acarretaria o enfraquecimento do grau de proteção que deve ser conferido a partir das normas constitucionais e legais aplicáveis ao caso, possibilitando abusos e acessos indevidos que poderiam ser inclusive escamoteados. Destaco, por último, que a permissão do acesso direto, pelas autoridades policiais, pode estimular que pressões indevidas sejam exercidas sobre os acusados para o fornecimento de senhas de acesso a informações confidenciais. [...] Penso, portanto, que o acesso aos aparelhos telefônicos deve ser submetido a prévia decisão judicial, na qual seja demonstrado, in concreto, a necessidade,

> adequação e proporcionalidade do acesso aos dados e informações requeridos. Trata-se de medida fundamental para resguardar os direitos individuais e evitar buscas genéricas (*fishing expedition*). Isso porque a necessidade de controle judicial impõe a demonstração da necessidade da medida e da sua justa causa, além de possibilitar o estabelecimento de limites aos dados a serem coletados.[101]

Sintetizando a questão jurídica posta no caso, a qual deu ensejo à instauração do Tema 977-STF, o Tribunal de Justiça do Rio de Janeiro absolveu o réu ao considerar ilegal a prova obtida após a apreensão de seu celular e acesso, por parte dos policiais, aos registros de chamadas e contatos sem autorização judicial.

A partir disso, o Ministério Público do Rio de Janeiro, discordando da decisão colegiada, recorreu ao Superior Tribunal de Justiça, argumentando que a ação se enquadra como apreensão de objetos essenciais para a comprovação do crime.

Irresignado, o Ministério Público interpôs recurso ao Supremo Tribunal Federal, oportunidade na qual o Ministro Dias Toffoli, na qualidade de relator, votou pelo provimento do recurso e consequente desconsideração da ilicitude das provas produzidas. Entretanto, os Ministros Edson Fachin e Gilmar Mendes divergiram da posição do relator, ressaltando a imprescindibilidade de decisão judicial fundamentada na adequação, necessidade e proporcionalidade em sentido estrito para o acesso aos dados obtidos em celular.

A partir de tais fundamentos, foi proposta a fixação da seguinte tese em repercussão geral:

> O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos (CF, art. 5º, X e XX).[102]

A tese estabelece que o acesso a informações armazenadas em aparelhos celulares apreendidos em locais de crime atribuídos a um suspeito requer uma decisão judicial prévia, sendo tal exigência fundamental para proteger os direitos fundamentais à

---

[101] BRASIL. Supremo Tribunal Federal. **ARE 1.042.075/RJ**. Rel. Ministro Gilmar Mendes. Tribunal Pleno, Brasília/DF. Em julgamento.

[102] Disponível no site oficial do Supremo Tribunal Federal: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5173898&numeroProcesso=1042075&classeProcesso=ARE&numeroTema=977

intimidade, privacidade e ao sigilo das comunicações e dados, conforme o artigo 5º, X e XX da Constituição Federal.

Isso significa que, antes da tomada de qualquer medida invasiva aos registros telefônicos, o que inclui os dados armazenados em nuvem, além, por exemplo, da agenda de contatos ou outros dados pessoais, é necessário que um juiz avalie e justifique, com base em evidências concretas, a necessidade, a adequação e a proporcionalidade em sentido estrito[103] dessa medida.

Além disso, estabelece a tese que essa decisão judicial deve delimitar claramente a abrangência do acesso, garantindo que a investigação não ultrapasse os limites legais e constitucionais, tudo visando evitar abusos e garantir que a coleta de dados não seja invasiva, respeitando os direitos individuais e evitando a prática da pescaria probatória ou *fishing expedition*.

Acerca dessa terminologia, Alexandre Morais da Rosa assim a conceitua:

> *Fishing Expedition* ou Pescaria Probatória é a procura especulativa, no ambiente físico ou digital, sem "causa provável", alvo definido, finalidade tangível ou para além dos limites autorizados (desvio de finalidade), de elementos capazes de atribuir responsabilidade penal a alguém. [...]
> Denomina-se pescaria (ou expedição) probatória a prática relativamente comum de se aproveitar dos espaços de exercício de poder para subverter a lógica das garantias constitucionais, vasculhando-se a intimidade, a vida privada, enfim, violando-se Direitos Fundamentais, para além dos limites legais. O termo se refere à incerteza própria das expedições de pesca, em que não se sabe, antecipadamente, se haverá peixe, nem os espécimes que podem ser fisgados, muito menos a quantidade, mas se tem "convicção" (o agente não tem provas, mas tem convicção). Com o uso de tecnologias (Processo Penal 4.0), cada vez mais se obtém a prova por meios escusos (especialmente em Unidades de Inteligência e/ou investigações paralelas, todas fora do controle das regras democráticas), requentando-se os "elementos obtidos às escuras" por meio de investigações de origem duvidosa, "encontro fortuito" dissimulado ou, ainda, por "denúncias anônimas *fakes*".[104]

Como observado, o excerto mencionado descreve a prática conhecida como *Fishing Expedition* ou Pescaria Probatória, que se refere à busca especulativa de provas, tanto no ambiente físico quanto digital, sem uma base legal sólida, vale dizer, sem "causa

---

[103] Acerca da regra da proporcionalidade, confira-se a lição doutrinária de Virgílio Afonso da Silva. SILVA, Virgílio Afonso da. **O Proporcional e o Razoável**. Revista dos Tribunais 798 (2002): 23-50. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/97313 Acesso em 01.11.2024

[104] ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico de acordo com a teoria dos jogos e MCDA-C**. 1. Ed. Florianópolis [SC]: Emais, 2021. P. 389 e 390.

provável", alvo definido ou objetivo claro, desviando-se dos limites legais e das garantias constitucionais a partir da invasão da privacidade e da intimidade das pessoas sem justificativa adequada.

Com isso, é válido afirmar que o acesso a aparelhos telefônicos por parte dos agentes policiais sem uma autorização judicial ou respaldada em uma decisão mal fundamentada caracteriza uma violação dos direitos fundamentais. Além disso, a terminologia já vem sendo utilizada pelo Superior Tribunal de Justiça, a exemplo do AgRg no HC n. 733.910/SC:

> [N]ão se pode admitir que a entrada na residência especificamente para o cumprimento de mandado de prisão sirva de salvo-conduto para que todo o seu interior seja vasculhado indistintamente, em verdadeira pescaria probatória (*fishing expedition*), sob pena de nulidade das provas colhidas por desvio de finalidade" (AgRg no HC n. 733.910/SC, relator Ministro Reynaldo Soares da Fonseca, Quinta Turma, julgado em 6/9/2022, DJe de 13/9/2022).[105]

No caso em comento, a 5ª Turma da Corte Cidadã ratificou a concessão da ordem de *habeas corpus* para reconhecer a prática de *fishing expedition* no domicílio do acusado, oportunidade na qual declarou a ilicitude de todas as provas obtidas no interior da residência, além das delas derivadas.

Nesse contexto, especificamente no âmbito da proteção dos dados telemáticos, convém ressaltar que, a partir do momento em que foi promulgado o Projeto de Emenda Constitucional 17/2020, a Emenda Constitucional 115 de 2022 incluiu no artigo 5º da Constituição da República o inciso LXXIX, segundo o qual "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.".

Como visto, tal dispositivo representa um avanço significativo no reconhecimento e na garantia dos direitos individuais no contexto digital. O artigo 5º, LXXIX, da Constituição, estabelece que todos têm o direito fundamental à proteção de seus dados pessoais, abrangendo tanto os meios tradicionais quanto os digitais, de modo que, em um mundo cada vez mais conectado e dependente da tecnologia, essa proteção se torna essencial para preservar a privacidade e a integridade dos cidadãos.

Como decorrente disso, a inclusão explícita da proteção de dados pessoais na Constituição reflete a necessidade de adaptação às novas realidades tecnológicas, onde

[105] Disponível em: https://scon.stj.jus.br/SCON/. Palavras-chave: "Fishing expedition".

informações pessoais são frequentemente coletadas, armazenadas e compartilhadas, especialmente na seara da investigação e persecução criminal.

Afinal, o direito concretizado pela nova redação não apenas resguarda a individualidade dos cidadãos, mas também impõe limites ao poder do Estado e de entidades privadas sobre informações sensíveis, garantindo que sejam tratadas de maneira ética, legal e transparente, para cuja violação é imprescindível autorização judicial bem fundamentada.

Dessarte, como explica Gabriela Felden Scheuermann, a proteção dos dados pessoais alcançou grau hierárquico constitucional:

> Nesse contexto, a PEC 17/2019 foi aprovada nas duas Casas do Congresso Nacional e se transformou na Emenda Constitucional nº 115 de 2022. Com isso, a partir de 2022 os dados pessoais passaram a ser protegidos não mais como uma extensão da privacidade e da intimidade, mas como um direito em si, isto é, um direito fundamental autônomo.
> Ao ser vista como um direito fundamental, a proteção de dados irradia por todas as relações, tanto sociais como jurídicas, exercendo influência direta na adequação para respeitar referido direito. Diante disso, quando se trata de direitos fundamentos como normas constitucionais, manifestamos a sua superioridade formal, sendo essa uma característica extremamente importante dos direitos fundamentais. E agora, os dados pessoais também possuem essa hierarquia constitucional.[106]

Como visto, a partir de 2022, os dados pessoais passaram a ser protegidos não apenas como parte do direito ao sigilo das comunicações, à privacidade e à intimidade - abarcados pelos incisos X e XII do artigo 5º da Constituição -, mas como um direito fundamental independente que alcançou hierarquia constitucional, tornando-se definitivamente um direito fundamental.

Assim, a partir do momento em que a proteção de dados é reconhecida como cláusula pétrea, sua importância se estende a todas as relações sociais e jurídicas, influenciando diretamente a forma como este direito deve ser respeitado e protegido. Dessa forma, considerando que os direitos fundamentais possuem superioridade hierárquica em relação aos demais direitos, os dados pessoais também gozam dessa hierarquia, gerando reflexos principalmente para o processo penal.

---

[106] SCHEUERMANN, Gabriela Felden. **Dados pessoais como um direito fundamental autônomo a partir da Emenda Constitucional nº 115/2022**. Revista da Defensoria Pública do Estado do Rio Grande do Sul, Porto Alegre, v. 2, n. 33, p. 253–274, 2023. P. 17 e 18. Disponível em: https://revistadpers.emnuvens.com.br/defensoria/article/view/600. Acesso em 04.10.2024

Durante a investigação criminal, os dados pessoais podem ser coletados para fins de análise e evidência, de modo que a nova redação constitucional atua como um baluarte contra abusos e violações dos direitos individuais, exigindo que esses dados sejam tratados de acordo com princípios éticos e legais, demandando a criação de novas normas infraconstitucionais com a finalidade de regular o direito fundamental previsto, tudo com a finalidade de se exigir fundamentações judiciais suficientes caso se pretenda o relativizar.

Acerca do dever de fundamentação das decisões judiciais, assim ensinam Gilmar Ferreira Mendes e Paulo Gustavo Gonet Branco:

> A garantia da proteção judicial efetiva impõe que tais decisões possam ser submetidas a um processo de controle, permitindo, inclusive, a eventual impugnação. Daí a necessidade de que as decisões judiciais sejam devidamente motivadas (CF, art. 93, IX). E motivar significa dar as razões pelas quais determinada decisão há de ser adotada, expor as suas justificações e motivos fático-jurídicos determinantes. A racionalidade e, dessa forma, a legitimidade da decisão perante os jurisdicionados decorrem da adequada fundamentação por meio das razões apropriadas.[107]

O trecho enfatiza que, para garantir a proteção judicial efetiva, é essencial que as decisões judiciais sejam passíveis de impugnação. Para isso, as decisões precisam ser bem fundamentadas, devendo conter as razões e justificativas, tanto fáticas quanto jurídicas, que as sustentam, pois a racionalidade e a legitimidade de uma decisão judicial dependem de fundamentação clara e adequada, demonstrando aos envolvidos no processo o porquê de determinada decisão ter sido tomada.

Isso, pois, além de proteger os indivíduos investigados, a garantia constitucional de proteção de dados também fortalece a confiança na justiça e no sistema jurídico como um todo. Ao assegurar que informações pessoais não sejam utilizadas de maneira inadequada, incumbe ao Poder Judiciário atuar de modo a evitar o vazamento indevido de dados ou o uso para outros fins não autorizados.

A problemática identificada neste ponto é que, conforme explica João Paulo Lordelo, a Lei Geral de Proteção de Dados, que estabelece regras para o tratamento de dados pessoais, tanto em plataformas digitais quanto físicas, realizadas por pessoas físicas

[107] MENDES, Gilmar Ferreira.; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 12 ed. São Paulo: Saraiva, 2015. P. 420.

ou por empresas e instituições públicas ou privadas, não é aplicável no âmbito da segurança pública e das investigações criminais:

> De forma similar ao ocorrido no âmbito europeu em 2016, a Lei nº 13.709/2018 (LGPD) disciplina, no Brasil, o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. De acordo com o seu art. 4º, essa Lei não se aplica ao tratamento de dados pessoais realizados para fins particulares e não econômico, para fins jornalísticos, artísticos, acadêmicos, bem como para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Há, portanto, uma relevante lacuna do tema no que diz respeito à persecução penal.[108]

Como explicado, a LGPD não se aplica a dados usados para fins pessoais sem objetivo econômico, ou para atividades jornalísticas, artísticas, acadêmicas, de segurança pública e investigações criminais, deixando lacunas protetivas inaceitáveis para o patamar tecnológico alcançado pela humanidade atualmente[109].

Dessa forma, porquanto inexistente regulamentação infraconstitucional no tocante ao acesso aos dados digitais para fins de investigação criminal, é imperiosa a criação de norma específica para regular o inciso LXXIX do artigo 5º da Constituição Federal no âmbito da apuração de crimes, incluindo, para além do *standard* probatório para acesso aos dados armazenados em nuvem, desde o armazenamento seguro até a restrição de acesso apenas a pessoal autorizado, assegurando a conformidade com os fins protetivos almejados pelo texto constitucional.

Desse modo, a proteção dos dados pessoais durante as investigações criminais não possui como objetivo apenas o resguardo dos direitos individuais, mas também promove a transparência e a equidade nos processos judiciais.

Conforme analisado, a Lei 12.965/14 estabelece um importante arcabouço jurídico para a proteção dos direitos dos usuários na esfera digital, enfatizando a privacidade, a proteção de dados pessoais e a liberdade de expressão. Ao criar diretrizes claras sobre o

---

[108] LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. 2.ed., rev. e atual. 2 São Paulo: Editora JusPodivm. 2024. P. 239-240.

[109] "Quando observamos o meio digital, observa-se que a forma de nos comunicarmos entre nós e transmitirmos informações mudou desde o final do século XX. Cada vez mais, a vida e m sociedade está permeada pela internet, com acesso a sites e aplicativos e, assim, deixando um rastro digital de arquivos, acessos e dados na rede mundial de computadores. De início, estamos lidando com sistemas de informática, o que corresponde, basicamente, ao tratamento automatizado de informações realizados por processadores presentes em computadores."*In*: SMANIO, op. cit. p. 51.

uso da internet no Brasil, a lei busca garantir que os direitos fundamentais sejam respeitados em um ambiente cada vez mais conectado.

Entretanto, o *standard* probatório previsto no Marco Civil ainda é insuficiente, especialmente no que diz respeito à fundamentação das decisões judiciais que autorizam o acesso a dados armazenados, decisões essas que não seguem o mesmo rigor dos requisitos previstos na Lei 9.296/96. Consequentemente, a falta de um padrão rigoroso para a quebra do sigilo telemático pode resultar em decisões arbitrárias, comprometendo a proteção da privacidade dos cidadãos.

Apesar de determinado segmento da jurisprudência brasileira estar tentando buscar um equilíbrio entre a necessidade de investigação e a proteção dos direitos individuais, como evidenciado em casos que abordam práticas de *fishing expedition* e a necessidade de conferir melhor fundamentação à quebra do sigilo telemático, o entendimento dominante ainda está longe de apresentar uma mudança significativa.

Portanto, a recente inclusão do inciso LXXIX no artigo 5º da Constituição Federal, que assegura o direito à proteção de dados pessoais, representa notório avanço na proteção dos direitos individuais no contexto digital, reforçando a importância de práticas robustas de segurança e proteção de dados, promovendo a confiança no sistema jurídico.

Por fim, considerando que o principal fator que confere legitimidade à prestação jurisdicional é justamente o rigor da fundamentação de suas decisões, a contínua adaptação da jurisprudência à realidade ora posta deve considerar os riscos de não conferir aos dados estáticos um grau protetivo equiparável às interceptações telefônicas.

3. *STANDARD* PROBATÓRIO DAS DECISÕES JUDICIAIS PARA O ACESSO AOS DADOS ARMAZENADOS EM NUVEM

A análise dos *standards* probatórios necessários para a proferimento de decisões judiciais que decretam medidas cautelares, especialmente no que tange à quebra do sigilo de dados eletrônicos armazenados em nuvem, é um tema de grande relevância no contexto jurídico contemporâneo, sobretudo diante do fato de que as informações probatórias mais relevantes para uma investigação criminal atualmente são encontradas nos novos meios de armazenamento de dados, e podem estar misturadas com conteúdo pessoais sensíveis abarcados por proteção constitucional (artigo 5º, LXIX, da CRFB).

Isso ocorre, pois a crescente digitalização das informações e a utilização de serviços de armazenamento em nuvem levantam questões complexas sobre a proteção da privacidade e a segurança jurídica, exigindo uma reflexão aprofundada sobre os critérios que devem ser utilizados para justificar tais intervenções.

No contexto das medidas cautelares, a quebra do sigilo de dados eletrônicos requer uma análise cuidadosa dos direitos fundamentais envolvidos, como o direito à privacidade e à proteção de dados pessoais. A jurisprudência brasileira, embora tenha avançado em algumas áreas, ainda carece de uma abordagem sistemática sobre os *standards* probatórios aplicáveis às situações de acesso aos dados digitais estáticos armazenados em nuvem.

A falta de clareza neste aspecto pode resultar em decisões que não respeitam os direitos dos indivíduos, gerando um déficit de justificação que compromete a legitimidade das intervenções estatais.

Deve-se ter em mente que o processo determina uma "reconstrução histórica dos fatos" a partir de rastros do passado, de maneira que a versão adotada refletirá tal história de um modo analógico, mas nunca integral, abrangente e inquestionável.[110]

De acordo com Gustavo Badaró, "meios de prova são os instrumentos pelos quais se leva ao processo um elemento de prova apto a revelar ao juiz a verdade de um fato"[111]. Servem, diretamente, para provar a veracidade da hipótese fática, para convencer o julgador. São exemplos as declarações do ofendido, os relatos das testemunhas, os documentos, dentre outros.

[110] KHALEDE JR, Salah H**. A busca da verdade no processo penal. Para além da ambição inquisitorial.** São Paulo: Atlas, 2013., p. 591.
[111] BADARÓ, Gustavo Henrique. **Epistemologia judiciária e prova penal.** São Paulo: Thomson Reuters Brasil, 2019.p. 677

Já os meios de obtenção de prova são meios de investigação; nas palavras daquele mesmo autor, são "instrumentos para a colheita de fontes ou elementos de prova"[112]. Não são provas, mas meios para obtê-las. Servem para recolher elementos que, conforme o resultado da medida, poderão constituir meios de prova. Como exemplos de meios de obtenção de prova, há as "quebras" de sigilos bancário, fiscal ou telefônico, a interceptação de comunicação telefônica, a gravação ambiental e a infiltração de agente. Também são denominadas medidas cautelares probatórias.

Seguindo esse entendimento, nesse tópico será analisado o instituto do "*Standard* probatório", buscando a compreensão conceitual para analisar os precedentes encampados pelo Superior Tribunal de Justiça no *Habeas Corpus* 444.024-PR (2018/0078245-6) e no Agravo Regimental no Recurso em Mandado de Segurança 71.168-RJ (2023/0124057-3).

Tais julgados foram escolhidos por serem os consolidarem o entendimento, no âmbito do Superior Tribunal de Justiça, da inaplicabilidade da Lei 9.296/96 à quebra de sigilo de dados armazenados.

3.1. Conceituação do termo "*Standard* probatório"

Como sabido, a fundamentação das decisões judiciais é uma exigência prevista no artigo 93, IX, da Constituição da República, o qual determina que toda decisão do Poder Judiciário deve ser devidamente motivada, impondo ao magistrado a obrigação de justificar suas decisões, demonstrando os fundamentos de fato e de direito que as sustentam. A ausência de fundamentação pode levar à nulidade da decisão, pois compromete a transparência e a legitimidade do processo judicial. A respeito, assim leciona Lenio Streck e Igor Raatz:

> O dever de fundamentação não pode ser encarado como um simples dever de justificação. O art. 93, IX, da Constituição Federal somente será respeitado quando o julgador se desincumbir do ônus de demonstrar que sua decisão é correta, que está fundada em prejuízos legítimos e que sua subjetividade não se sobrepôs ao direito a sua história institucional, levando-se em consideração o contexto circunstancial dos fatos definidor do caso concreto. Com efeito, não se encontrará cumprido o dever de fundamentação somente com a menção a critérios lógicos, sendo

[112] Idem. p. 678

> indispensável colocar o sentido ventilado na decisão no contexto da história institucional do direito.[113]

Como explicado pelos autores, para que o dever de fundamentação seja efetivamente cumprido, é necessário que o juiz exponha de maneira clara como sua decisão se insere dentro da "história institucional" do direito, isto é, como ela está alinhada com os precedentes, os princípios e as normas que regem o sistema jurídico. O contexto fático e jurídico deve ser levado em consideração, de modo que a decisão esteja em sintonia com os valores e objetivos do ordenamento jurídico, e não apenas com argumentos lógicos isolados.

Em outras palavras, a fundamentação deve ir além da justificação teórica, sendo preciso demonstrar que o resultado alcançado é legítimo tanto em termos jurídicos quanto práticos, devendo o julgador detalhar como os elementos probatórios foram aplicados à situação específica, evidenciando que a decisão é fruto de um processo reflexivo.

Nesse contexto, como corolário da fundamentação de qualquer decisão judicial, o termo "*standard probatório*" diz respeito ao padrão de prova necessário para que um juiz ou tribunal considere uma alegação como suficientemente comprovada para a finalidade de proferir uma decisão judicial que limite determinada garantia legal ou fundamental em prol de um objetivo maior. Esse conceito é central no processo penal, pois define o grau de certeza - de *prova* - exigido para que uma decisão limitadora de direitos seja tomada.

Assim, o "*standard*" de prova é um critério utilizado para verificar se as evidências apresentadas alcançam o nível necessário para fundamentar a decisão judicial. Segundo Janaina Matida e Antonio Vieira:

> A referência ao termo *standard de prova* tem sido, nos últimos anos, cada vez mais comum quando se discorre sobre temas probatórios, no âmbito do direito processual brasileiro. De fato, tanto na doutrina como na práxis forense, cada vez mais autores e operadores jurídicos recorrem à expressão para designar critérios de suficiência probatória, os quais, no campo do processo penal, permitiriam saber quando há prova suficiente para proferir uma decisão condenatória e quando, pelo contrário, estaria o magistrado obrigado a absolver o réu por não haver alcançado um mínimo probatório necessário para a desfecho de condenação.[114]

---

[113] STRECK, Lenio Luiz; RAATZ, Igor. **O Dever de Fundamentação das Decisões Judiciais sob o Olhar da Crítica Hermenêutica Do Direito**. Revista Opinião Jurídica, vol. 15, núm. 20, julio, 2017, pp. 160-179. Centro Universitário Christus Ceará, Brasil. P. 169. Disponível em: https://www.redalyc.org/articulo.oa?id=633868963015 Acesso em 16.10.2024

[114] MATIDA, Janaina; VIEIRA, Antonio. **Para além do BARD: uma crítica à crescente adoção do standard de prova "para além de toda a dúvida razoável" no processo penal brasileiro**. Revista Brasileira de Ciências Criminais, v. 156. 2019. P. 222.

Embora o trecho se limite à hipótese de sentenças condenatórias ou absolutórias em processos criminais, é certo que há diferentes níveis de *standards* probatórios, os quais variam de acordo com a gravidade da decisão a ser tomada. Por exemplo, em casos criminais, o nível de prova exigido é mais alto do que em casos civis, pois envolve a liberdade do réu. Por sua vez, no processo penal, o *standard* mais utilizado é o da "prova além da dúvida razoável"[115], aplicável nos casos de condenação.

Isto porque, ao consagrar a presunção de inocência e seu subprincípio *in dubio pro reo*, a Constituição Federal e a Convenção Americana sinalizam claramente na adoção do *standard* probatório de "além da dúvida razoável", que, somente se preenchido, autoriza um juízo condenatório.

Destaca-se que a partir da matriz teórica anglo-saxão, são estabelecidos os seguintes padrões probatórios (*standards):* prova clara e convincente (*clear and convincing evidence*); prova mais provável que sua negação (*more probable than not);* preponderância da prova (*preponderance of the evidence*); e prova além da dúvida razoável (*beyond a reasonable doubt).*

O mais exigente deles é o "além da dúvida razoável"[116] (*beyond a reasonable doubt)*, sendo, portanto, o utilizado na sentença penal. É por isso que o CPP fala em

---

[115] "Isso quer dizer que um standard mais rigoroso, como o "além da dúvida razoável", ocasiona que exista uma segurança no sentido de que serão evitados ao máximo casos em que se considere como provados fatos que, em realidade, não ocorreram. Entre o erro de se declarar como provado um fato que não ocorreu ou não se aceitar o reconhecimento de algo que efetivamente tenha acontecido, opta-se por assentar que o sistema judicial deve se estruturar para evitar afirmar fatos falsos como verdadeiros". *In*: VASCONCELLOS, Vinícius Gomes de. **Standard probatório para condenação e dúvida razoável no processo penal: análise das possíveis contribuições ao ordenamento brasileiro**. Revista Direito GV, v. 16, n. 2, 2020. P. 6. Disponível em: https://doi.org/10.1590/2317-6172201961

[116] Foi em meados dos anos 90 que o critério da prova além da dúvida razoável passou a ser mencionado por juízes das cortes brasileiras. No julgamento do HC 73.338/RJ pelo Supremo Tribunal Federal, impetrado num caso de acusação de prática do crime de corrupção de menores (art. 1º da Lei nº 2.252/1954), o relator do *writ*, Ministro Celso de Mello, para afastar a caracterização de tal figura típica e conceder parcialmente a ordem, asseverou que cumpria ao Ministério Público "demonstrar, de modo consistente – e além de qualquer dúvida razoável – a ocorrência do fato constitutivo do pedido, comprovando documentalmente a condição etária (menor de 18 anos) da vítima (...)". No ano de 2007, o referido ministro, no julgamento do HC 83.947/AM, que questionava uma acusação de prática de um crime financeiro (art. 25 da Lei nº 7.492/1986), reiterou tal compreensão ao conceder a ordem, salientando que "nenhuma acusação penal se presume provada. Não compete, ao réu, demonstrar a sua inocência. Cabe, ao contrário, ao Ministério Público, comprovar, de forma inequívoca, para além de qualquer dúvida razoável, a culpabilidade do acusado" (destaques no original). Esse entendimento também foi manifestado no voto que Celso de Mello proferiu na condição de relator do HC 84580/AM, julgado em 25/08/2009 (DJe 18/09/2009). Entretanto, nesses dois casos o referido ministro mencionou o BARD para justificar a rejeição da denúncia. E antes foi demonstrado que o critério norte-americano para guiar o exame de admissibilidade da denúncia é a *probable causa. Cf: BRASIL. Supremo Tribunal Federal. HC 73.338/RJ. Relator(a): Min. Celso de Melo. Brasília/DF, 13/08/1996. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=74424. Acesso em:* 06/12/2024. BRASIL. Supremo Tribunal Federal. HC 83.947/AM. Relator(a): Min. Celso de Melo. Brasília/DF,

indícios razoáveis ou indícios suficientes para decisões interlocutórias com menor exigência probatória.

Sobre esse aspecto, há possibilidade de se estabelecer um grau de exigência probatória variável com base na fase processual em que o caso se encontra, em virtude da referência do Código de Processo Penal a "indícios razoáveis e indícios suficientes". Esse ajuste no padrão de exigência pode ser ilustrado, por exemplo, pela significativa diferença entre o nível de prova necessário para decretar uma medida cautelar em comparação com o requerido para proferir uma sentença condenatória.

Nesse contexto, especificamente no tocante às medidas cautelares, no âmbito da Lei 9.296/96 - Lei de Interceptação Telefônica -, o *standard* de prova exigido para autorizar que sejam interceptadas conversas telefônicas e telemáticas em andamento consistem em não haver "indícios razoáveis da autoria ou participação em infração penal" (artigo 2º, I); e a prova não puder "ser feita por outros meios disponíveis" (artigo 2º, II), sendo imperiosa a presença de fundamentação judicial no sentido de que todos os outros meios probatórios subsidiários sejam insuficientes para alcançar a prova que se pretende obter.[117]

Os indícios, em essência, constituem provas mais frágeis, insuficientes para sustentar um veredito condenatório, mas que podem ser adequadas para embasar determinadas decisões judiciais, como, por exemplo, o recebimento de uma denúncia ou a pronúncia. Portanto, ao permitir decisões com base em indícios, ocorre um ajuste descendente do padrão probatório estabelecido pela exigência de "prova além da dúvida razoável", de maneira logicamente consistente.[118]

Dependendo da fase do processo, não é imprescindível que seja aplicado um padrão que exija um grau extremamente alto de probabilidade, como é o caso das sentenças de mérito. Um exemplo disso é a prisão temporária, que requer apenas fundamentadas razões de autoria, conforme estabelecido no artigo 1º, III, da Lei nº

07/08/2007. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=506601 Acesso em: 06/12/2024.

[117] "A exigência de indícios razoáveis de autoria ou participação em infração penal (cf. art. 2º, I) deixa clara a presença do fumus boni iuris como primeiro pressuposto da medida cumulada com a inexistência de outros meios de prova disponíveis para a obtenção das informações necessárias, representando, assim, o *periculum in mora*. Neste último caso, evidencia-se a necessidade e a urgência da medida. Posto isto, não temos dúvidas em afirmarmos que a natureza jurídica da medida de interceptação telefônica é CAUTELAR. Portanto, de índole normativa processual." *In*: RANGEL, Paulo. **Breves considerações sobre a Lei 9.296/96 - Interceptação telefônica**. Revista do Ministério Público, Rio de Janeiro, RJ, (6), 1997. P. 179.

[118] LOPES JUNIOR, Aury; ROSA, Alexandre Morais da. **Sobre o uso do standard probatório no processo penal. 2019**. Disponível em: https://www.conjur.com.br/2019-jul-26/limitepenal-uso-standard-probatorio-processo-penal. Acesso em: 01 mar. 2025.

7.960/1989, enquanto a prisão preventiva exige indícios suficientes de autoria, conforme estabelecido no artigo 312 do Código de Processo Penal.

Da mesma forma, no caso de sequestro, é necessário apenas indícios fortes de origem ilícita dos bens, conforme estipulado no artigo 126 do Código de Processo Penal. Nessas situações, é possível identificar variações nos níveis de probabilidade exigidos, que vão desde uma simples preponderância até uma probabilidade consideravelmente maior. Portanto, quando se trata de decisões que não são sentenças de mérito, outros modelos de avaliação podem ser aplicados, que não demandam a exigência de "prova além da dúvida razoável".

O afastamento judicial de sigilo de dados telefônicos (detalhamento ou histórico das ligações) pode se dar sempre que necessário para se tentar elucidar fatos atinentes ao cometimento de um ilícito penal. Nesses casos, em que se almeja a quebra dos sigilos de dados, são bem leves os parâmetros de exigência para se autorizar tais medidas, bastando que seja retratada a "necessidade para a apuração" ou o "interesse da justiça" e a disposição de elucidar os fatos a partir de indícios de possível prática delitiva.

Esses são critérios que devem orientar a tomada da decisão no sentido do deferimento ou do indeferimento da medida cautelar voltada à colheita de elemento de prova. Note-se que, malgrado as referidas leis silenciem, é evidente que tal necessidade ou interesse deve estar calcado em indícios da materialidade delitiva e em indícios, ainda que tênues, de autoria ou da participação na prática criminosa.[119] Não fosse assim, estaria aberta uma perigosa janela para a violação de direitos fundamentais sem uma justificativa plausível.

Por outro lado, em relação às interceptações de comunicações telefônicas ou de comunicações via sistemas de informática e telemática para fins de investigação ou instrução criminal, a Lei nº 9.296/1996 exige que a autoridade requerente da medida aponte "indícios razoáveis da autoria ou participação" em infração penal punida com reclusão. Essa exigência "não pode ser confundida com a mera suspeita, que pode decorrer, de uma simples conjectura pessoal, sem amparo em nenhum dado objetivo de

[119] Como assinala Madeira Dezem, o "indício", o "indício suficiente" e o "indício razoável" são standards probatórios "que não são de fácil diferenciação" (DEZEM, Guilherme Madeira. **Curso de Processo Penal.** 4. ed. São Paulo: Revista dos Tribunais, 2018, p. 832). Porém, pode-se notar que os adjetivos têm o propósito de retratar o maior grau de corroboração da hipótese fática que é esperado em determinada situação ou contexto.

conhecimento".[120]Também é necessário que a prova dos fatos não possa ser produzida por outros meios (caráter de subsidiariedade).

Como essa medida cautelar probatória é mais invasiva, representando uma maior restrição a direitos fundamentais, a lei estabelece um *standard* um pouco mais pesado, mais exigente, reclamando que a autoridade policial ou o agente do Ministério Público indiquem "indícios razoáveis" de que o representado está cometendo determinado delito e que não há outra maneira de coletar as provas da ilicitude que está em andamento[121].

Esse padrão de suficiência probatória está acima do que é exigido para a decretação das quebras de sigilo referidas nos parágrafos anteriores, mas, claramente, aquém da justa causa, que é o *standard* que orienta o juízo de admissibilidade da denúncia.

No caso da quebra de sigilo de dados armazenados em nuvem, o artigo 22 do Marco Civil da Internet trata da possibilidade de uma parte interessada, seja em um processo civil ou penal, solicitar ao juiz o acesso a registros de conexão e de acesso a aplicações de internet.

O parágrafo único do artigo define os requisitos (*standards*) que devem ser cumpridos para que o pedido seja aceito. Primeiro, é necessário haver indícios concretos de que ocorreu um ato ilícito. Segundo, a parte deve justificar claramente os motivos de os registros solicitados serem relevantes para a investigação ou para a produção de provas. Por último, deve ser especificado o período de tempo ao qual os registros solicitados se referem, garantindo a precisão e pertinência da solicitação.

Ocorre que, diferentemente da Lei de Interceptação Telefônica, o Marco Civil da Internet não prevê a necessidade de o magistrado indicar a insuficiência dos demais meios de prova para alcançar a finalidade almejada, refletindo em evidente vulnerabilidade dos dados armazenados em detrimento das comunicações em andamento.[122]

---

[120] GRINOVER, Ada Pellegrini. Provas ilícitas, interceptações e escutas. Brasília: Gazeta, 2013, p. 516

[121] Como aduziu Schietti Cruz, "com efeito, a interceptação telefônica atinge uma das liberdades mais importantes do indivíduo, que é a livre expressão do pensamento externado durante a comunicação, que pode portar os segredos mais íntimos da pessoa humana ou, como explicita José Afonso da Silva, "confissões íntimas, na confiança que se deu pura confidência" (Comentário Contextual à Constituição. São Paulo: Malheiros Editoria, 2006, p. 104). Diversamente ocorre com o sigilo bancário, cujas informações pessoais são estáticas, em regra unipessoais, referentes a movimentações financeiras e de conhecimento das instituições financeiras e de inúmeras pessoas (funcionários, gerentes, escriturários etc), cujo acesso somente não é franqueado ao público de maneira geral" (BRASIL. Superior Tribunal de Justiça. HC 349.945/PE, Relator(a): Min. Nefi Cordeiro, Rel. p/ Acórdão Min. Rogerio Schietti Cruz, 6ª Turma, julgado em 06/12/2016, DJe 02/02/2017. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201600498873&dt_publicacao=02/02/2017. Acesso em: 03.04.2025.

[122] "No campo legislativo, não se vislumbra a proposição de normas que possam conferir solução jurídica aos problemas surgidos com as provas digitais, no que se relaciona à classificação das provas, seu procedimento, seu valor probatório, os limites de sua utilização, dentre outros. O Marco Civil da Internet,

Por conseguinte, a necessidade de um *standard* probatório claro e bem definido é ainda mais evidente em casos que envolvem a quebra de sigilo de dados eletrônicos armazenados em nuvem, porquanto as informações constantes nessa modalidade de armazenamento podem ser muito mais sensíveis do que aquelas captadas a partir do fluxo de comunicações telefônicas e telemáticas.

O *standard* refere-se a padrões que apontam uma demarcação, um mínimo probatório que deve ser superado para que se considere um fato como provado. Em termos diretos, eles definem o "quanto de prova" (nível de suficiência probatória ou grau de confirmação).[123] Existem diversos *standards* probatórios possíveis, conforme o grau de dificuldade que se imponha para se aceitar um fato como provado. A definição do *standard* de prova, portanto, é uma escolha política e valorativa.

Nos domínios do processo penal, como se pôde observar, os critérios de suficiência probatória variam de acordo com o tipo de provimento jurisdicional requestado e conforme o momento ou fase processual.

Em suma, a discussão sobre os *standards* probatórios necessários para a proferimento de decisões judiciais que decretam medidas cautelares, especialmente no que se refere à quebra do sigilo de dados eletrônicos, é um tema que demanda uma análise cuidadosa e aprofundada. A construção de um arcabouço teórico sólido, que considere as especificidades do contexto digital e os direitos fundamentais envolvidos, é essencial para garantir a efetividade e a legitimidade das intervenções estatais.

Projeto de Lei nº 2.126/2011, disciplina o uso da internet e prevê os direitos dos usuários. Com referência a provas, porém, somente dispõe sobre a requisição judicial de registros de conexão e registros de acesso. A questão do registro e preservação dos dados também é objeto do Projeto de Lei nº 5.403/2001, que aguarda votação na Câmara dos Deputados." *In*: VAZ, Denise Provasi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório**. 2012. Tese (Doutorado em Direito Processual) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. P. 16. Disponível em: https://doi.org/10.11606/T.2.2012.tde-28052013-153123. Acesso em 01.11.2024

[123] KIRCHER, Luís Felipe S. **O convencimento judicial e os parâmetros de controle sobre o juízo de fato: visão geral, direito comparado e o Tribunal Penal Internacional**. Revista Due In Altum, v. 10, n. 20, p. 179-206, jan./abr. 2018. https://doi.org/10.22293/2179-507x.v10i20.692.

3.2. O *Habeas Corpus* 444.024-PR (2018/0078245-6) e a consolidação do entendimento da inaplicabilidade da Lei 9.296/96 à quebra de sigilo de dados armazenados

No âmbito do *Habeas Corpus* 444.024-PR (2018/0078245-6)[124], o Superior Tribunal de Justiça teve a oportunidade de se debruçar a respeito da (in)aplicabilidade por analogia da Lei 9.296/96 às decisões judiciais que tratam do acesso aos dados estáticos armazenados em dispositivos locais ou externos (nuvem).

Tratava-se de investigação que se concentrava em apurar supostas irregularidades na contratação de obras públicas pela Concessionária da Rodovia Osório-Porto Alegre S.A. (Concepa). O inquérito policial foi instaurado para investigar a contratação de obras para a 4ª faixa da BR 290-RS, que, segundo o Ministério Público Federal, ocorreu sem o devido processo licitatório, levantando preocupações sobre a legalidade da operação.

O Ministério Público requereu ao Juízo da 11ª Vara Federal da Seção Judiciária de Porto Alegre/RS a expedição de mandado de busca e apreensão que deveria ser executado nas instalações das empresas envolvidas, assim como na casa dos réus. O objeto do mandado incluía:

> [...] apreender valores de procedência não comprovada e documentos relacionados à execução e produtos do crime em questão, bem assim computadores, telefones celulares, notebooks, hard disc (HD), pen-drives, cds, dvds e quaisquer outras mídias de armazenamento,além de qualquer elemento que constitua prova da prática de outro crime.[125]

Diante dessa conjuntura, a defesa impetrou *Habeas Corpus* no Tribunal Regional Federal da 4ª Região, que denegou a ordem. Sendo opostos Embargos de Declaração pela defesa, que foram rejeitados.

Assim, a banca de advogados impetrou outro remédio constitucional ao Superior Tribunal de Justiça, argumentando que não havia justificativa válida para permitir, por força do mandado de busca e apreensão, o acesso aos dados dos dispositivos que foram apreendidos.

---

[124] BRASIL. Superior Tribunal de Justiça. ***Habeas Corpus* 444.024-PR (2018/0078245-6)**. Rel. Min. Sebastião Reis Jr.. Rel. P. Acórdão Min. Rogerio Schietti Cruz. 6ª Turma, Brasília/DF, DJ 02.08.2019. Disponível em: https://scon.stj.jus.br/SCON/. Palavras-chave: "mídias"; "Lei n. 12.965/2014"; "acesso"; "informações"; "dados estáticos".

[125] Op. Cit. Inteiro teor, p. 16.

Sustentaram os impetrantes que a decisão do Juízo deveria estar concreta e especificamente motivada sobre a adequação (artigo 22, I, da Lei 12.965/14), a necessidade (artigo 22, II, da Lei 12.965/14) e a proporcionalidade (artigo 22, III, da Lei 12.965/14) da medida, alegando que a autorização foi dada de forma totalmente genérica, configurando *fishing expedition*.

Segundo a tese apresentada, a decisão violaria as disposições das Leis 12.965/14 e 9.296/96, além de contrariar a jurisprudência estabelecida na Corte. E, com fundamento nos requisitos da Lei 9.296/96, argumentaram que a decisão não considerou a possibilidade de obter as informações necessárias para a investigação por métodos menos invasivos, como, por exemplo, o envio de ofício aos réus ou à empresa onde trabalham.

O relator do caso, Ministro Sebastião Reis Júnior, abordou a questão da fundamentação necessária para a autorização de busca e apreensão de dados armazenados em dispositivos eletrônicos, como celulares e computadores, à luz das leis que regulam a privacidade e o sigilo das comunicações. No voto (vencido), foi destacada a importância de se respeitar os direitos constitucionais e legais que garantem a inviolabilidade das comunicações, conforme estabelecido na Lei 12.965/14 e na Lei 9.296/96, que trata da interceptação de comunicações.

O Ministro argumentou que, para que a quebra do sigilo de dados armazenados em aparelhos eletrônicos seja considerada legal, é necessário que haja uma decisão judicial fundamentada que demonstre indícios razoáveis de autoria ou participação em um crime, que a prova não possa ser obtida por outros meios, além de que o crime investigado seja punido com pena de reclusão.

Menciona em seu voto que, mesmo na ausência de lei específica que defina os requisitos para a quebra do sigilo de aparelhos apreendidos, o Tribunal tem aplicado os princípios da Lei 9.296/96 por analogia, exigindo que a autorização judicial para acessar dados armazenados em dispositivos eletrônicos siga os mesmos critérios:

> Há um quadro (fl. 56), é verdade, na representação policial, em que há indicação das pessoas e empresas investigadas e em que há a menção dos pacientes apenas esclarecendo que o primeiro é presidente de uma das empresas investigadas e o outro é sócio-administrador do consórcio envolvido e diretor da empresa investigada. Os indícios razoáveis de autoria ou participação dos pacientes nos fatos objeto da investigação em curso não foram apresentados como exige o art. 2º, I, da Lei n. 9.296/1996.A decisão, alhures reproduzida, no que se refere ao acesso aos equipamentos apreendidos, é silente quanto a tais circunstâncias, citando apenas doutrina a qual afirma que o direito à privacidade não é absoluto, o que não se discute nos presentes autos. Não há referência a

> nenhum elemento diretamente ligado ao caso concreto. E não adianta dizer que houve a indicação dos pacientes quando do acolhimento do pedido de busca e apreensão. Primeiro, porque esse cuidou apenas em descrever os fatos investigados, nada dizendo quanto aos indícios que ligam os pacientes a tais fatos; nem quanto à impossibilidade de a investigação prosseguir sem o uso desse meio de prova; nem quanto à relevância das informações a serem obtidas com o acesso ao conteúdo dos equipamentos apreendidos para o caso concreto ou mesmo o período a ser investigado (um ano,dois, três, quatro, cinco, seis anos?). Nesse ponto, aliás, a ordem judicial é aberta,deixando ao arbítrio do investigador o período de acesso à privacidade dos investigados. E segundo, porque a busca e apreensão trouxe novas provas, cujas análises podem levar a conclusões diversas: ou afastar de vez as suspeitas sobre um ou mais investigados, tornando desnecessária essa prova mais invasiva; e apresentar elementos que justifiquem a prova; ou, por fim, apresentar elementos suficientes quanto à participação e responsabilidade dos investigados que tornem desnecessária.[126]

Como narrado, o contexto do caso envolvia a apreensão de dispositivos eletrônicos durante o cumprimento de mandado judicial, onde a autoridade policial buscava acessar todos dados estáticos que poderiam servir como prova, acesso esse autorizado por decisão judicial que não aplicou os requisitos da Lei 9.296/96.

No trecho mencionado, o Ministro Sebastião Reis argumenta que a decisão judicial que autorizou o acesso aos dados armazenados em aparelhos eletrônicos não atendeu aos requisitos legais necessários, conforme estabelecido no artigo 2º, I e II, da Lei 9.296/96, o qual não admite a quebra nas hipóteses em que “a prova puder ser feita por outros meios disponíveis” (artigo 2º, II).

O Ministro observa que, embora a representação policial tenha mencionado as pessoas e empresas investigadas, não foram apresentadas evidências concretas que ligassem os pacientes (as pessoas cujos dados estavam sendo solicitados) aos fatos da investigação. A decisão judicial foi criticada por ser "silente" ao não trazer informações específicas que demonstrassem a necessidade de acessar os dados dos investigados.

Ademais, foi ressaltado o fato de que a mera menção de que um dos pacientes é presidente de uma empresa investigada e o outro é sócio-administrador não é suficiente para justificar a invasão de sua privacidade, tendo sido posteriormente destacado que a decisão não abordou a impossibilidade de prosseguir com a investigação por outros meios de prova, e tampouco demonstrou a relevância das informações que seriam obtidas com o acesso aos dados.

[126] Op. Cit. Inteiro teor, p. 20 e 21.

Não obstante, foi criticada a falta de clareza sobre o período de tempo que os dados abrangeriam, o que deixaria a decisão aberta e sujeita ao critério do investigador, potencialmente permitindo um acesso excessivo à privacidade dos investigados.

Ao final de seu voto, o relator ressaltou que a busca e apreensão já havia gerado novas provas que poderiam ser analisadas para, inclusive, afastar as suspeitas sobre os investigados, demonstrando que, antes de recorrer a uma medida tão invasiva quanto a quebra de sigilo de dados, seria prudente avaliar as novas evidências obtidas e considerar se realmente era necessário acessar os dados dos aparelhos.

Ao adotar tais critérios, orientou-se o voto relator em regras rígidas para a quebra do sigilo de dados telemáticos, na esteira de como defendem Raquel Scalcon e André da Rocha Ferreira:

> Quanto às quebras de sigilo de dados pessoais contra um pessoa individualizada ou contra um grupo de pessoas claramente pré-delimitado, alguns critérios mínimos devem ser adotados: (i) a adequação da jurisprudência criminal do País de modo a respeitar o direito fundamental à proteção de dados, iniciando-se pelo abandono do termo "dado armazenado" e pela adoção do conceito de "dado pessoal", fazendo com que os princípios inerentes à matéria sejam incorporados em qualquer procedimento criminal que envolva dados pessoais; (ii) o dado ou metadado em si que o Estado pretende obter com a quebra deve estar entre aqueles cuja utilização, para fins de persecução penal, está legalmente autorizada; (iii) a decisão deve garantir o respeito aos princípios da proteção de dados, notadamente os trazidos pela LGPD, inclusive devendo haver adequação das agências de segurança para tanto; e, (iv) além de outros princípios de Direito Penal, deve haver atenção para a existência de *fumus delicti comissi* (e periculum in mora) por parte de cada titular do dado pessoal, com justificação da efetividade da medida para o caso concreto.[127]

Com isso, a ordem foi parcialmente concedida para decretar a nulidade da decisão apenas no tocante à autorização da quebra do sigilo de dados. Após, o Ministro Rogério Schietti Cruz pediu vista dos autos, tendo proferido seu voto no sentido de reconhecer a licitude da quebra do sigilo telemático e denegar a ordem.

Ao inaugurar a divergência, o Ministro apresenta uma análise detalhada sobre a inaplicabilidade, ao caso, da Lei 9.296/96, que regula a interceptação de comunicações, justificando os motivos pelos quais não considerou apropriada a aplicação por analogia dessa lei para o acesso a dados estáticos.

---

[127] SCALCON, Raquel; FERREIRA, André da Rocha. **O problema da quebra coletiva de sigilo de dados pessoais contra pessoas indeterminadas**. Boletim IBCCRIM 31, no. 370 (2023): 18-20. P. 20.

Um dos principais fundamentos utilizados no voto divergente para afastar a aplicação por analogia da Lei 9.296/96 é a distinção entre a interceptação de comunicações e o acesso a dados armazenados. O Ministro Rogério Schietti argumenta que a lei foi criada com um foco específico na proteção do sigilo das comunicações em tempo real, enquanto o acesso aos dados armazenados envolve questões diferentes de privacidade e proteção de informações.

No voto divergente, foi enfatizado que a Lei 12.965/14 já estabelece diretrizes claras sobre a proteção de dados pessoais e a privacidade na internet, argumentando que essa legislação é mais adequada para regular o acesso a dados armazenados, pois aborda diretamente as questões de privacidade e a proteção de informações pessoais em ambientes digitais.

Em contrapartida ao voto proferido pelo relator, o Ministro Rogério Schietti discute a necessidade de se estabelecer limites claros para o acesso a dados armazenados em equipamentos eletrônicos apreendidos, porém limita as diretrizes legislativas à luz do Marco Civil da Internet. Em seu voto, foi mencionado o artigo 10 do Marco Civil da Internet, que trata da guarda e disponibilização de registros de conexão e de acesso a às aplicações de internet[128].

Este artigo estabelece que a preservação da intimidade, da vida privada, da honra e da imagem das partes envolvidas deve ser respeitada pelos provedores, os quais apenas poderão relativizar tais direitos mediante decisão judicial que não necessariamente precisa conter os padrões estabelecidos pela Lei 9.296/96.

O parágrafo 2º do artigo 10 da Lei 12.965/14 é particularmente relevante, pois determina que o conteúdo das comunicações privadas só pode ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, "respeitado o disposto nos incisos II e III do artigo 7º". Isso implica que, para acessar dados que possam conter informações privadas, é necessário um respaldo legal que justifique tal medida, respaldo esse que não requer maior aprofundamento como faz a Lei de Interceptações Telefônicas.

Além disso, o artigo 22 do Marco Civil da Internet é citado de modo a estabelecer diretrizes para a quebra de dados armazenados. Nos termos da divergência,

[128] "Registros de conexão são os registros que ficam sob a guarda das empresas de telecomunicação, que permitem o acesso à internet e estão relacionados com o número de IP e momento em que uma determinada conexão de internet se iniciou. Registros de acesso a aplicações de internet são os metadados referentes à utilização de serviços on-line (Google, redes sociais, demais aplicativos).". Op. Cit. inteiro teor.

primeiramente, é necessária a existência de fundados indícios de um ilícito, isto é, deve haver evidências mínimas que indiquem que um crime foi cometido.

Em segundo lugar, a parte que faz o pedido deve apresentar justificativa motivada que demonstre a utilidade dos registros solicitados para fins de investigação ou para a formação de um conjunto probatório. Isso implica que a solicitação não pode ser feita de forma aleatória ou especulativa, mas, deve estar claramente vinculada à necessidade de elucidar um fato ou circunstância relevante para o processo.

Por fim, restou consignado que o pedido deve especificar o período ao qual se referem os registros, garantindo que a requisição seja precisa e delimitada no tempo. A partir de tais parâmetros, é mencionado no voto divergente que o mandado de busca e apreensão delimitou o acesso aos dados "apenas as mídias e as memórias em que estão os dados relativos ao crime, sendo desnecessária a guarda de todo o hardware dos computadores tipo desktop e notebook", tendo sido tal justificativa utilizada para afastar qualquer alegação de pescaria probatória.

O Marco Civil da Internet, segundo o Ministro, oferece um arcabouço legal que deve ser seguido em detrimento de uma legislação que não foi projetada para esse fim, qual seja, a Lei 9.296/96. Sua argumentação se coaduna com a doutrina de João Paulo Lordelo Guimarães Tavares, que, ao diferenciar os dados armazenados em nuvem ou nos discos rígidos das comunicações em andamento, sejam estas telefônicas ou telemáticas, defende a aplicação de legislações distintas:

> Embora o Marco Civil da Internet discipline a guarda e a exibição de dados de conexão – no caso dos provedores de conexão (art. 13, § 5º) – e de acesso – no caso dos provedores de aplicações de internet (art. 15, § 1º) –, existem outros dados igualmente relevantes, que podem ser fornecidos especialmente pelos provedores de aplicações de internet. Cuida-se de dados que, embora também possam ser compreendidos, genericamente,como dados telemáticos – no caso de aplicação para smartphone – ou informáticos – ser utilizado outro tipo de terminal –, não dizem respeito apenas à conexão à internet ou acesso a uma determinada aplicação. Curiosamente, o Marco Civil da Internet não parece se preocupar com essas informações, concentrando-se a Lei 12.965/2014 (LGL\2014\3339) em disciplinar dados pessoais relativos à conexão à internet – a exemplo do endereço IP, data e hora do acesso, além da porta lógica, no caso do uso de ferramenta NAT – e de acesso às aplicações – notadamente endereço IP, data, hora e duração do acesso. O que dizer de dados como as informações cadastrais em uma determinada rede social ou até mesmo o conteúdo de mensagens privadas de chat ou de e-mail? Certamente, não se trata de dados de conexão ou de acesso, mas são igualmente relevantes para fins probatórios. No que diz respeito aos dados cadastrais, a lei confere uma proteção menor ao seu acesso, sendo

> permitida, por exemplo, a requisição direta por membros do Ministério Público ou por autoridades policiais, desde que limitados a informações referentes à qualificação pessoal, à filiação e ao endereço (inclusive eletrônico) do usuário (art. 10-A,§ 1º, II, c/c arts. 15 a 17 da Lei 12.850/2013 (LGL\2013\7484); art. 10, § 3º, da Lei 12.965/2014 (LGL\2014\3339)). No caso de particulares ou outros órgãos públicos, a requisição desses dados dependerá de prévia autorização judicial. Por seu turno, o acesso ao conteúdo de documentos e conversas armazenados em aplicativos – a exemplo de mensagens de e-mail, mensagens de aplicativos de comunicação instantânea, documentos e conteúdos armazenados na nuvem, dados de localização, dados relativos à utilização de aplicações de serviços de transporte (Uber, 99 POP etc.), entre outros – deve sempre ser objeto de requerimento judicial prévio, da mesma forma que ocorre com documentos físicos ou correspondências obtidos por meio de busca e apreensão. E mais: na hipótese de interceptação do fluxo desses dados, ou seja, quando o que se deseja é o acesso simultâneo aos dados produzidos, será aplicado o regime das interceptações telefônicas (art. 1º, parágrafo único, da Lei 9.296/1996(LGL\1996\65)).[129]

O referido trecho diferencia as hipóteses de aplicabilidade da Lei 9.296/96 e do Marco Civil da Internet, ressaltando que, embora este trate da guarda e exibição de dados de conexão (para provedores de conexão, conforme o artigo 13, § 5º) e de acesso (para provedores de aplicações de internet, conforme o art. 15, § 1º), existem outros dados igualmente importantes, os quais podem ser fornecidos por provedores de aplicações de internet e incluem informações telemáticas ou informáticas que vão além da simples conexão à internet ou acesso a uma aplicação. O Marco Civil, no entanto, foca em regular dados pessoais relacionados à conexão e ao uso de aplicações, como o endereço IP, data, hora e duração do acesso.

Além disso, o texto levanta a questão sobre dados cadastrais, como informações de redes sociais ou conteúdo de mensagens privadas, que não se enquadram como dados de conexão ou acesso, mas são igualmente importantes para fins probatórios. Nesse caso, o acesso a esses dados é menos protegido pela lei e pode ser solicitado diretamente por autoridades como o Ministério Público ou a polícia, desde que seja limitado a dados pessoais como qualificação, filiação e endereço do usuário. Em contraste, para outros órgãos ou particulares, há a necessidade de autorização judicial prévia.

Especificamente no que diz respeito ao conteúdo de documentos e conversas em aplicativos, o texto deixa claro que é necessária autorização judicial para acesso, de forma

[129] TAVARES, João Paulo Lordelo Guimarães. **O regime jurídico das provas digitais no direito brasileiro**. Revista de Processo. vol. 316. ano 46. p. 373-387.São Paulo: Ed. RT, junho 2021. Disponível em: https://civilprocedurereview.com/revista/article/view/217

semelhante ao tratamento dado a documentos físicos. Já para interceptações simultâneas de dados, aplica-se o regime da interceptação telefônica, conforme a Lei 9.296/96.

Neste subtópico, a divergência entre os votos dos Ministros Sebastião Reis e Rogério Schietti reflete uma profunda discussão sobre a aplicabilidade da Lei 9.296/96 no contexto do acesso a dados armazenados. O voto do relator enfatizou a necessidade de uma fundamentação robusta para a autorização da quebra do sigilo de dados, argumentando que a decisão judicial deve demonstrar indícios razoáveis de autoria ou participação nos crimes investigados, além da demonstração do esgotamento das outras vias investigativas para que seja autorizada a invasão.

Sustentou, com isso, a aplicação por analogia da Lei 9.296/96, considerando a possibilidade de métodos menos invasivos para a obtenção de informações. Por outro lado, o Ministro Rogério Schietti apresentou um voto divergente que questionou a adequação da aplicação da Lei de Interceptações Telefônicas ao acesso a dados estáticos, argumentando que a legislação foi criada com foco na interceptação de comunicações em tempo real.

O voto divergente defendeu que o Marco Civil da Internet oferece diretrizes mais apropriadas para regular o acesso a dados armazenados, uma vez que aborda diretamente as questões de privacidade e proteção de informações pessoais em ambientes digitais. Sua análise, apoiada pela doutrina de especialistas como João Paulo Lordelo Guimarães Tavares, sugere que a distinção entre dados em trânsito e dados armazenados - ou estáticos - é crucial para a construção de um arcabouço legal que respeite os direitos fundamentais no contexto digital atual.

3.3. Análise do Agravo Regimental no Recurso em Mandado de Segurança 71.168-RJ (2023/0124057-3)

Conforme enfatizado até o momento, a questão dos *standards* probatórios para a decretação da quebra do sigilo de dados estáticos armazenados em nuvem ainda está longe de ser consolidada na jurisprudência brasileira. De um lado, verificam-se os requisitos bem delimitados da Lei 9.296/96 para as interceptações telefônicas e, de outro, a Lei 12.965/14 deixa a desejar principalmente no tocante à prescindibilidade de demonstração de que a prova pode ser feita por outros meios disponíveis.

Nesse contexto, embora não se possa afirmar que a Lei 9.296/96 é aplicável aos dados armazenados em nuvem, a definição de critérios para a referida quebra de sigilo foi

bem discutida no Agravo Regimental no Recurso em Mandado de Segurança 71.168-RJ, o qual se passará a analisar neste subtópico.

Nos registros do referido processo, está documentado que o Juízo da Vara Única da Comarca de Italva-RJ, no decorrer de um inquérito policial instaurado para apurar crime de roubo circunstanciado ocorrido em 22.05.2022, atendeu ao pedido de quebra de sigilo de dados telemáticos formulado pelo Delegado de Polícia responsável.

O magistrado, então, autorizou a quebra do sigilo de dados telemáticos de todos os usuários que, possivelmente, utilizaram os serviços da empresa [G. B. I. L. e G. LLC] em um raio de 500 (quinhentos) metros das coordenadas geográficas Latitude -21.427792"S e Longitude -41.549641"W, durante o intervalo entre 18:00 e 22:00 do dia 22.05.2022. O objeto da quebra não incluía somente os registros de conexão[130], mas também:

> [...] autorizou acesso amplo e irrestrito a: conteúdo armazenado associados às contas Google; conteúdo de Gmail; conteúdo do Google Fotos (incluindo os respectivos metadados – geomarcação); conteúdo do Google Drive; lista de contatos; histórico de localização, incluindo os trajetos pesquisados no google maps, waze e outros que importem a função GPS; consultas (pesquisas) realizadas pelo usuário do dispositivo (histórico de navegação/pesquisa); e, informações relacionadas às contas do Google Play, incluindo APPs baixados (downloads) ou comprados, lista de desejos, pessoas e informações relacionadas às contas referidas.[131]

Em razão disso, foi impetrado Mandado de Segurança no Tribunal de Justiça do Rio de Janeiro, o qual denegou a segurança sob o argumento de que a "Medida deferida que se mostra adequada, necessária e proporcional à hipótese investigativa em curso, sem excesso"[132]. Deste acórdão, foi interposto Recurso Ordinário ao Superior Tribunal de Justiça, o qual, em decisão monocrática proferida pela Ministra Laurita Vaz, desproveu o recurso.

No julgamento do Agravo Regimental no dia 16.05.2023, após o voto da relatora negando provimento, acompanhada pelo Ministro Rogerio Schietti Cruz, houve voto

---

[130] O art. 4º, VI, da Lei 12.965/14 define os registros de conexão como: "*o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;*"

[131] BRASIL. Superior Tribunal de Justiça. **AgRg no RMS 71.168-RJ (2023/0124057-3)**. Rel. Min. Laurita Vaz. Rel. P. Acórdão Min. Jesuíno Rissato (desembargador convocado). 6ª Turma, Brasília/DF, DJ 30.08.2023. Disponível em: https://scon.stj.jus.br/SCON/. Palavras-chave: "registro de conexão"; "Lei n. 12.965/2014"; "histórico de navegação". Inteiro teor, p. 16.

[132] Op. Cit. P. 7.

divergente do Ministro Sebastião Reis Júnior, que concedeu parcial provimento ao recurso. Em seguida, o Ministro Jesuíno Rissato (Desembargador convocado do TJDFT) solicitou vista do processo.

Continuado o julgamento em sessão ocorrida no dia 08.08.2023, após o voto vista do Ministro Jesuíno Rissato, que concedeu parcial provimento ao agravo regimental, acompanhado pelo Ministro Antônio Saldanha Palheiro, além da reconsideração do voto da relatora e do Ministro Rogerio Schietti Cruz na mesma linha, a Sexta Turma, de forma unânime, decidiu dar parcial provimento ao agravo regimental para restringir a quebra de sigilo de dados telemáticos apenas aos usuários que, possivelmente, utilizaram os serviços das agravantes dentro da área e do período especificados na decisão anterior, limitando-se exclusivamente aos registros de conexão e acesso às aplicações de internet[133], excluindo o acesso amplo e irrestrito a conteúdo das contas Google[134].

Em seu voto-vista, o Ministro Jesuíno Rissato buscou esclarecer a importância de equilibrar a atividade investigativa do Estado com a proteção dos direitos fundamentais dos indivíduos. Foi enfatizado que, embora a investigação seja uma função essencial do Estado, não se pode permitir que essa atividade ocorra de maneira ilimitada, sem respeitar os limites impostos pela legislação e pela Constituição.

Em observância aos incisos I, II e III do artigo 22 do Marco Civil da Internet, a Corte adotou o critério de que o magistrado (i) deve apresentar indícios que sugiram a prática de um crime, justificando a necessidade de acessar os dados; (ii) deve explicar como os dados requisitados são relevantes para a investigação em curso, demonstrando a utilidade da medida; e (iii) a decisão que autoriza a invasão deve ser específica quanto ao período de tempo em que os dados foram coletados, evitando solicitações amplas e genéricas que possam violar a privacidade de usuários inocentes.

Tal conclusão vai de encontro ao que foi estipulado pela doutrina de Gianluca Martins Smanio:

> Situação diametralmente oposta encontra-se nos dados e arquivos armazenados em servidores externos à máquina do indivíduo, como servidores de webmail, sistemas de nuvem, por exemplo, que podem ser acessados remotamente. Como o mandado de busca e apreensão domiciliar possui localização exata da medida restritiva a ser realizada, não pode conter descrições genéricas. Dessa maneira, apenas o dado e os

[133] O art. 4º, VIII, da Lei 12.965/14 define os registros de acesso a aplicações de internet como: "o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP."
[134] Op. Cit. P. 18.

> arquivos presentes naquele endereço podem ser alvo de busca e apreensão. Isso não quer dizer que tais dados não possam ser acessados pelos agentes policiais, desde que haja ordem judicial específica para o endereço da localidade dos servidores externos, ou que o acesso remoto esteja abrangido em decisão judicial, com especificidade quanto ao procedimento. Com o Marco Civil da Internet, a responsabilidade do provedor de serviços e aplicações de Internet foi positivada, exigindo deveres de proteção à intimidade e privacidade do detentor desses dados. Por estarmos diante de direitos fundamentais, a lei exige autorização judicial para que os agentes solicitem dados e arquivos pessoais do usuário a esses provedores, que, respeitando os ditames legais e os princípios constitucionais, mediante ordem judicial, podem entregá-los às autoridades para fins de investigação.[135]

Como observado, embora o autor diferencie a apreensão de dados armazenados localmente e aqueles guardados em servidores externos, como em serviços de *webmail* e nuvem, o mandado de busca e apreensão domiciliar - equiparado à autorização de quebra de sigilo do conteúdo armazenado nas contas do Google - apenas permite o acesso aos arquivos presentes no local específico descrito, não abrangendo dados em servidores remotos.

Para que os dados externos sejam acessados, é necessária uma ordem judicial especificamente fundamentada, detalhando o procedimento e o endereço dos servidores, pois o Marco Civil da Internet regula a atuação dos provedores, impondo a responsabilidade de proteger a privacidade e a intimidade dos usuários, implicando que a entrega de dados pessoais às autoridades só pode ocorrer mediante autorização judicial que respeite os *standards* probatórios previstos nos artigos. 7º, 22 e 23 da Lei 12.965/14.

Ademais, no acórdão do Agravo Regimental no Recurso de Mandado de Segurança 71.168-RJ, concluiu-se que não se pode considerar como registros de conexão ou de acesso a conteúdo de e-mails, fotos, vídeos ou qualquer outro tipo de informação que revele a vida íntima dos usuários, sejam eles armazenados em servidores externos (nuvem) ou no disco rígido de cada aparelho.

No voto vencedor, foi criticada a amplitude das medidas decretadas contra os investigados, tendo sido afirmado que elas ultrapassam o que é permitido pela legislação vigente, especificamente os artigos 22 e 23 da Lei 12.965/14, que trata do Marco Civil da Internet. O acórdão destaca que a lei define de forma clara o que se entende por "registros de conexão" e "registros de acesso a aplicações de internet", limitando tais definições a

[135] SMANIO, op. cit. p. 175.

informações específicas, como data, hora, duração da conexão e endereço IP (*internet protocol address*).

Por conseguinte, os dados pessoais, como conteúdos de e-mails, histórico de localização e informações de contas em serviços como Google, por representarem a vida privada dos indivíduos, não podem ser acessados de forma indiscriminada sem fundamentação proporcional e condizente, sendo bastante objetivo no sentido de que a legislação não faz menção ao acesso a tais informações, o que reforça a ideia de que a quebra de sigilo deve ser limitada aos elementos que realmente se enquadrem nas definições legais.

Especificamente no tocante aos "registros de conexão" e aos "registros de acesso a aplicações de internet", referentes aos IP's cujo acesso foi autorizado pelo Superior Tribunal de Justiça, vale mencionar que o Supremo Tribunal Federal, no âmbito do Recurso Extraordinário 1.301.250/RJ (*leading case*), instaurou o Tema 1.148, cujo título trata *dos "Limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas."*[136]

Assim está redigida a ementa que reconheceu a repercussão geral:

> DIREITO CONSTITUCIONAL. DIREITO PROCESSUAL PENAL. QUEBRA DE SIGILO DE DADOS PESSOAIS. REGISTROS DE ACESSO À INTERNET E FORNECIMENTO DE IP. DECISÃO GENÉRICA. NÃO INDICAÇÃO DE PARÂMETROS MÍNIMOS PARA IDENTIFICAÇÃO DOS USUÁRIOS. NÃO DELIMITAÇÃO, ADEMAIS, DO ESPAÇO TERRITORIAL EM QUE VEICULADA A ORDEM. PROTEÇÃO À INTIMIDADE E AO SIGILO DE DADOS (ART. 5º, X e XII, CF). QUESTÃO CONSTITUCIONAL. POTENCIAL MULTIPLICADOR DA CONTROVÉRSIA. REPERCUSSÃO GERAL RECONHECIDA. 1. Possui índole constitucional e repercussão geral a controvérsia relativa aos limites e ao alcance de decisões judiciais de quebra de sigilo de dados pessoais, nas quais determinado o fornecimento de registros de acesso à internet e de IPs (internet protocol address), circunscritos a um lapso temporal demarcado, sem, contudo, a indicação de qualquer elemento concreto apto a identificar os usuários. 2. Repercussão geral reconhecida. (RE 1301250 RG, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 27-05-2021, PROCESSO ELETRÔNICO DJe-108 DIVULG 07-06-2021 PUBLIC 08-06-2021)[137]

[136] STF. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/tema.asp?num=1148

[137] STF. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvance=true&classeNumeroIncidente=RE%201301250

No caso concreto do *leading case*, trata-se de Recurso Extraordinário derivado de Mandado de Segurança impetrado pela Google Brasil Internet LTDA no âmbito da investigação do homicídio da Vereadora Marielle Franco. O ato apontado como coator foi proferido pelo Juízo da 4ª Vara Criminal do Rio de Janeiro, o qual determinou a quebra de sigilo telemático de todos os usuários não identificados que realizaram pesquisas no Google utilizando as palavras-chave "Marielle Franco", "casa das pretas" e "rua dos inválidos" durante os quatro dias subsequentes ao crime (14.03.2018).

No corpo da ação, a pessoa jurídica Google LTDA sustenta que a prática de realizar varreduras amplas nos históricos de pesquisa dos usuários e fornecer listas temáticas das pessoas que buscaram determinadas informações constitui violação ao direito à privacidade, especialmente quando essas ações não estão relacionadas ao crime investigado.

Reconhecida a repercussão geral, a Ministra Rosa Weber, em sessão virtual iniciada em 22.09.2023, proferiu voto dando provimento ao Recurso Extraordinário no sentido da proibição da quebra de sigilo dos dados telemáticos de um grupo de pessoas não identificadas no decorrer de investigação criminal.

Na oportunidade, foi proposta a seguinte tese: "À luz dos direitos fundamentais à privacidade, à proteção dos dados pessoais ao devido processo legal, o artigo 22 da Lei 12.965/2014 (Marco Civil da Internet) não ampara ordem judicial genérica e não individualizada de fornecimento dos registros de conexão e de acesso que, em lapso temporal demarcado, tenham pesquisado vocábulos ou expressões específicas em provedores de aplicação". Até o momento, o julgamento não foi concluído.

Como visto, o Tema 1.148 de repercussão geral do Supremo Tribunal Federal trata dos limites para decretação judicial da quebra de sigilo de dados telemáticos, especificamente no âmbito de procedimentos penais e em relação a pessoas indeterminadas. A questão discute até que ponto é constitucional a autorização judicial para a quebra de sigilo de comunicações telemáticas (como e-mails e mensagens instantâneas), quando não há uma definição clara das pessoas investigadas.

O Tema envolve a interpretação dos incisos X e XII do artigo 5º da Constituição Federal, que protegem a intimidade, a vida privada e o sigilo das comunicações. A título informativo, o Tema também aborda o art. 93, IX[138], que trata da fundamentação das

[138] "Descrição: Recurso extraordinário em que se discute, à luz da Constituição Federal, artigos 5º, X e XII, e 93, IX, a constitucionalidade de decreto judicial genérico de quebra de sigilo de dados telemáticos, para efeito de divulgação de informações pessoais de usuários indeterminados, sem a respectiva identificação,

decisões judiciais, evidenciando a preocupação da Suprema Corte em estipular um padrão mínimo de fundamentação judicial para a decretação da quebra de sigilo dos dados telemáticos, dos registros de conexão e dos registros de acesso a aplicações de internet (artigo 7º, VII, e art. 20 da Lei 12.965/14).

Nesse contexto, considerando que o entendimento adotado pelo Superior Tribunal de Justiça no Agravo Regimental no Recurso em Mandado de Segurança 71.168-RJ seja uma defesa à necessidade de um equilíbrio entre a atividade investigativa do Estado e a proteção dos direitos fundamentais dos cidadãos, os *standards* probatórios lá estabelecidos poderão ser complementados pelo Supremo Tribunal Federal de forma mais específica aos "registros de conexão" e aos "registros de acesso a aplicações de internet", cuja autorização para acesso foi concedida pela Corte Cidadã.

Em conclusão, o julgamento do Agravo Regimental no Recurso em Mandado de Segurança 71.168-RJ demonstrou a importância de equilibrar as necessidades da investigação estatal com a proteção dos direitos fundamentais à privacidade e à intimidade. A decisão da Sexta Turma do Superior Tribunal de Justiça de restringir a quebra de sigilo aos registros de conexão e acesso a aplicações de internet, excluindo o acesso irrestrito a conteúdos pessoais armazenados, evidencia a cautela necessária em casos de coleta de dados telemáticos, em especial no tocante à necessidade de suficiência da fundamentação para o acesso aos dados armazenados em dispositivos locais ou externos (nuvem), tendo em vista a sensibilidade das informações que poderão ser acessadas.

4. PROPOSTAS PARA ELABORAÇÃO DE PROJETO DE LEI

No contexto da crescente digitalização das informações e da necessidade de proteção dos direitos fundamentais dos indivíduos, a elaboração de um projeto de lei que regule a quebra do sigilo de dados armazenados em dispositivos locais ou externos (nuvem) se torna uma urgência inadiável. A ausência de uma legislação federal específica que trate desse tema, especialmente à luz da Lei 9.296/96, inaplicável ao caso, e da Lei 12.965/14, concebida para causas cíveis, gera lacunas que podem comprometer tanto a eficácia das investigações criminais quanto a proteção da privacidade dos cidadãos.

considerada a proteção constitucional da intimidade e da vida privada.”. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/tema.asp?num=1148

Assim, este capítulo propõe diretrizes legislativas que visam estabelecer um marco jurídico claro e rigoroso para a autorização judicial da quebra do sigilo de dados estáticos, assegurando a segurança jurídica e a proteção dos direitos dos investigados.

Em primeiro plano, é imprescindível que a questão seja regulada por Lei Federal (artigo 22, I, da CRFB[139])[140], sobretudo para assegurar a eficácia do artigo 5º, X, XII e LXXIX, da Constituição da República, cujo grau de abstração abre margem para decisões judiciais arbitrárias, afetando a segurança jurídica.

A partir disso, a redação legal deve exigir para a quebra do sigilo de dados armazenados em nuvem uma decisão judicial fundamentada, que se baseie em indícios mínimos de autoria e materialidade. Não obstante, faz-se necessário que a fundamentação seja robusta, demonstrando que a medida é imprescindível para a elucidação dos fatos e que não existem alternativas menos invasivas que possam ser utilizadas para a obtenção das informações desejadas, semelhantemente ao que já é utilizado pela Lei 9.296/96:

> Da necessidade de uma regulamentação, em especial, da parte final do inciso XII do art. 5º da CF, sobreveio a Lei nº 9.296/96, conhecida como Lei de Interceptação Telefônica, base legal para solicitações judiciais de interceptações do fluxo de comunicações telefônicas. Esta norma regula a quebra de sigilo telefônico e foi concebida com uma norma de excepcionalidade, estipulando os casos em que a quebra do sigilo não será admitida: (a) quando houver indícios razoáveis da autoria ou participação em infração penal; (b) nos casos em que a prova puder ser feita por outros meios disponíveis; e (c) quando o fato que está sendo investigado constituir infração penal punida com pena máxima de detenção. A regulamentação da matéria opta, claramente, por um critério de proporcionalidade na utilização do meio (escuta telefônica) restritivo da privacidade do indivíduo, à medida que implica o emprego excepcional da escuta, i.e., somente para crimes mais graves, assim considerados aqueles punidos com pena de reclusão, e somente quando outros meios não forem suficientes para a prova da autoria ou participação em atividade criminosa. Não poderia ser de outro modo: tratando-se a privacidade e o correlato sigilo das comunicações telefônicas de um direito fundamental, sua restrição deve operar-se na estrita medida necessária (princípio da proibição do excesso) e de modo

[139] Art. 22. Compete privativamente à União legislar sobre: I - direito civil, comercial, penal, processual, eleitoral, agrário, marítimo, aeronáutico, espacial e do trabalho;

[140] "A fonte imediata do Direito Penal é puramente a lei. Não se trata de simples limitação à matéria jurídica em apreço, mas em verdadeira obediência à separação dos poderes e à própria legalidade em sentido estrito. No Brasil, o constituinte originário delegou privativamente à União competência para legislar acerca de Direito Penal (artigo 22, inciso I, CRFB/88), impedindo determinadamente a delegação de tal atribuição a outro ente federativo. Qualquer pretensa lei penal oriunda da administração estará incuravelmente maculada pela inconstitucionalidade." GUZZO, Matheus Muniz. **A Violação do Princípio da Legalidade pelas Normas Penais em Branco: uma Visão Sistematizada do Estatuto do Desarmamento**. Revista do Ministério Público do Rio de Janeiro nº 67, jan./mar. 2018. P. 185. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/124374 Acesso em 15.10.2024

> adequado, necessário e proporcional em sentido estrito (princípio da proporcionalidade). O princípio da proporcionalidade tem servido ao Poder Judiciário como instrumento para o controle dos atos do poder público que restringem direitos fundamentais, como é o caso da norma que regulamenta a parte final do inciso XII do art. 5º da CF/88.[141]

Dessa forma, a inadmissibilidade da prova obtida sem a devida demonstração de que meios menos invasivos foram considerados deve ser um princípio norteador, assegurando que a privacidade do indivíduo seja respeitada e também abrindo margem para a finalidade investigativa.

Além disso, a redação legal deve prever a necessidade de prévia identificação do crime investigado e do suposto autor do crime, sendo esta fundamental para que a decisão judicial não se baseie em suposições ou conjecturas, mas em elementos concretos envolvendo a mínima delimitação dos fatos a serem objeto da quebra do sigilo. O objetivo dessa disposição é justamente evitar a busca exploratória, muitas vezes decretada a partir de coordenadas geográficas, ainda que por período determinado:

> A principal crítica feita à ordem de quebra de sigilo com base em coordenadas geográficas, ou *geofence warrant*, é a ausência de identificação prévia dos suspeitos cujos dados serão quebrados. Argumenta-se que esse tipo de medida seria uma verdadeira quebra de sigilo exploratória, sem alvos individualizados, não albergada pela ordem jurídica brasileira.[142]

Nesse contexto, é possível abrir uma exceção para os casos nos quais a própria natureza do crime investigado não permita a imediata identificação dos envolvidos. Assim, na impossibilidade de se identificar o autor, o dispositivo legal deve exigir a apresentação de elementos concretos que demonstrem a prática de crimes no ambiente virtual por pessoas anônimas. Essa abordagem não apenas protege a privacidade dos indivíduos, mas também contribui para a eficiência das investigações, evitando a coleta excessiva de dados que não tenham relação direta com a investigação em curso.

---

[141] ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. **A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência**. Revista de Investigações Constitucionais 4, no. 3 (2019): 167-200. p. 15. Disponível em: https://doi.org/10.5380/rinc.v4i3.51295 Acesso em 01.11.2024

[142] MAIA, Tiago Dias; PAULINO, Galtiênio da Cruz. **A quebra de sigilo de dados baseada em coordenadas geográficas e o princípio da proporcionalidade.** Escola Superior do Ministério Público da União. P. 778. Disponível em: https://escola.mpu.mp.br/publicacoes/obras-avulsas/e-books-esmpu/direitos-fundamentais-em-processo-2013-estudos-em-comemoracao-aos-20-anos-da-escola-superior-do-ministerio-publico-da-uniao/44_a-quebra-de-sigilo-de-dados.pdf

Menciona-se, a título de exemplo, o Recurso em Mandado de Segurança 61.419/SE, impetrado pela empresa Google para questionar decisão do Tribunal de Justiça do Estado de Sergipe. Neste caso, a Corte sergipana havia determinado a quebra de sigilo telemático de um conjunto não identificado de pessoas que estavam em uma localização geográfica específica durante um determinado período.

A Google impugnou a decisão, argumentando que a quebra de sigilo violava direitos fundamentais, especialmente o direito à privacidade. Entretanto, o Superior Tribunal de Justiça denegou a segurança. Primeiramente, a Corte reconheceu a existência de um interesse público relevante que justificava a quebra do sigilo telemático, pois a investigação estava relacionada a crimes de organização criminosa e homicídio, e a necessidade de apurar esses delitos foi considerada mais importante do que a proteção da privacidade dos usuários afetados.

Neste caso, o Ministro Sebastião Reis Júnior, na qualidade de relator, destacou que, de acordo com o Marco Civil da Internet, os dados de acesso e de localização são considerados dados pessoais. Ele argumentou que, conforme o artigo 22 do Marco Civil, as autoridades judiciais têm a prerrogativa de requisitar esses dados em processos criminais, mesmo que os alvos da investigação não estejam previamente identificados, contanto que a requisição seja feita desde que os dados sejam "identificáveis".

Assim, a autorização para a identificação reversa dos suspeitos foi fundamentada na necessidade de investigação criminal, respeitando os princípios do Marco Civil da Internet, que permite a quebra de sigilo em situações onde há um interesse público relevante e a fundamentação adequada por parte do Judiciário[143].

[143] "Por outro lado, no RMS 61.419/SE, de relatoria do ministro Sebastião Reis Júnior, no exercício da presidência do STJ, julgado em 31 de julho de 2019, a Corte Federal se debruçou diante do recurso ordinário constitucional em mandado de segurança impetrado pela Google contra acórdão do Tribunal de Justiça do Estado de Sergipe,que manteve a ordem de quebra de sigilo telemático de conjunto não identificado de pessoas que estariam unidas por transitarem em de-terminada localização geográfica em definido espaço de tempo, especificando, a decisão na origem, requerer os dados de IPs dos usuários da aplicação em determinado local e hora. A liminar, no entanto, não foi concedida. Primeiramente, o ministro especifica que a medida, na verdade, é caso de busca por localização reversa que envolve quebra de sigilo de dados pessoais, sendo parte deles registros de acesso a aplicações de internet, e não se trata de interceptação telemática. O ministro categoriza os dados relativos ao momento de acesso enquanto regis-tro de acesso a aplicações da internet, nos termos do artigo 5º, VIII,do Marco Civil da Internet, e os dados de localização enquanto dados pessoais, nos termos do artigo 14, I, do Regulamento do Marco Civil Da Internet. Uma vez que trata-se de requisição de dados pessoais, é possível aduzir da decisão proferida pelo ministro que nos termos do Marco Civil da Internet, segundo o artigo 22, combinado com o artigo 10, §1º, que os dados de conexão em conjunto com dados pessoais podem ser requisitados por autoridade judicial em curso de processo criminal, não exigindo a lei que os potenciais alvos da quebra estejam identificados, bastando que os dados sejam identificáveis." 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

Superado este ponto, a proposta legislativa deve também estabelecer regras claras sobre a cadeia de custódia da prova digital coletada, devendo ser previsto que a integridade dos dados deve ser mantida por meio da utilização de algoritmos *hash*[144] ou outra ferramenta que garanta que as informações não sejam alteradas durante o processo de coleta e análise.

Ademais, a inviolabilidade do local de armazenamento dos dados deve ser assegurada, estabelecendo que apenas profissionais qualificados e autorizados possam acessar e manipular as informações[145], a fim de evitar o vazamento de informações íntimas que sejam totalmente desconexas com o objeto do crime investigado.

Outro aspecto relevante a ser considerado na proposta legislativa é a limitação do uso das provas coletadas apenas às informações que sejam relevantes para o objeto da investigação. Isso implica que, uma vez autorizada a quebra do sigilo, o acesso às informações deve ser restrito ao que é estritamente necessário para a apuração dos fatos, evitando a coleta desmedida de dados que podem dificultar a análise dos arquivos relevantes.

Ademais, a proposta deve contemplar a criação de mecanismos de supervisão e controle acerca do cumprimento das decisões judiciais que autorizam a quebra do sigilo de dados. A implementação de um sistema que permita a verificação do cumprimento do que foi especificamente disposto na decisão judicial é essencial para garantir a transparência e a *accountability* no uso de medidas que afetam a privacidade dos cidadãos.

Brasileira de Ciências Policiais, Brasília, Brasil, v. 12, n. 5, p. 49–76, 2021. Disponível em: https://dspace.mj.gov.br/handle/1/7921 . P. 66. Acesso em 08.11.2024

144 "Além da análise do aparelho utilizado, o uso da função hash é fundamental para assegurar a integridade dos dados lógicos colhidos, periciados durante o manejo do dispositivo informático pelos órgãos investigatórios. Tal código ou função é, de maneira bem simplificada, gerado por um algoritmo utilizado para mapear dados e criar uma identificação única do arquivo periciado. Uma vez gerado o código, é criada uma "impressão digital" do arquivo, de forma que a mudança de um bit que seja resulta na geração de um novo código, garantido a lisura da evidência. Esse procedimento é indispensável para deixar clara a exata correspondência entre os arquivos de mídia utilizados em juízo e os que correspondem aos captados no mundo físico." OLIVEIRA, Lurã Azevedo de; MEDINA, Lucas Arieh Bezerra. **A cadeia de custódia das provas colhidas em aparelhos móveis de gravação**. Boletim IBCCRIM, [S. l.], v. 31, n. 364, p. 16–19, 2024. P. 18. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1584 Acesso em 08.11.2024

145 "Permissões são atributos que controlam o acesso a arquivos e diretórios de um sistema computacional. As permissões podem ser de leitura, escrita e execução e cada usuário terá diferentes níveis de acesso em relação aos vários arquivos diretórios do sistema. Diferentes usuários de um sistema terão níveis de permissão diversos para cada arquivo. Suponhamos um arquivo de texto qualquer armazenado em um sistema computacional. Outros terão permissão de leitura e escrita, podendo lê-lo e modificá-lo (acrescentar, modificar ou mesmo apagar conteúdo). Haverá ainda aqueles sem qualquer permissão de acesso e estes não poderão nem lê-lo nem alterá-lo." VIANNA, Tulio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de direito penal informático**. Repositório UFMG. Dissertação de Mestrado. 2001. P. 85 e 86. Disponível em: http://hdl.handle.net/1843/BUOS-96MPWG Acesso em 10.11.2024

Nesse caso, a supervisão deve ser realizada por agentes independentes capazes de avaliar a conformidade das ações com o que foi fixado na decisão.

Não obstante, a legislação deve também prever penalidades administrativas e criminais específicas aos agentes encarregados da investigação que ultrapassarem o objeto do que foi autorizado, incorrendo em *fishing expedition*.

Embora os artigos. 25 e 26 da Lei 13.859/19 - Lei de Abuso de Autoridade - prescrevam as práticas de "Proceder à obtenção de prova, em procedimento de investigação ou fiscalização, por meio manifestamente ilícito" e "Requisitar instauração ou instaurar procedimento investigatório de infração penal ou administrativa, em desfavor de alguém, à falta de qualquer indício da prática de crime, de ilícito funcional ou de infração administrativa", nenhuma destas disposições é específica em relação ao desvio de finalidade do objeto das investigações.

Outra proposta interessante é a criação de um canal de comunicação entre os provedores de serviços de armazenamento em nuvem e as autoridades competentes (Ministério Público Estadual, Federal, Polícias Judiciárias Civis e Polícia Federal). Esse canal deve permitir que os provedores sejam notificados sobre as decisões judiciais que autorizam a quebra do sigilo de dados, garantindo que as informações sejam fornecidas de forma rápida e eficiente, sobretudo garantindo a cadeia de custódia das informações.

Em suma, a elaboração de um projeto de lei que regule a quebra do sigilo de dados em nuvem deve ser pautada pela necessidade de proteção dos direitos individuais, pela exigência de um *standard* probatório mínimo e pela implementação de regras claras sobre a coleta e o uso das provas digitais. A construção de um arcabouço jurídico sólido e que respeite direitos fundamentais é essencial para garantir a efetividade das investigações, ao mesmo tempo em que se preserva a confiança da sociedade no sistema de justiça.

CONCLUSÃO

Sem pretender esgotar as discussões sobre o tema, esta dissertação teve como intento proporcionar uma análise detalhada e crítica sobre a intersecção entre tecnologia, direito e investigação criminal. Ao longo dos capítulos, foram abordados temas fundamentais que revelam a complexidade e a urgência de se estabelecer um marco legal adequado para o acesso a dados estáticos armazenados em dispositivos internos e externos (nuvem).

No primeiro capítulo, foi discutida a evolução da sociedade da informação e o impacto das tecnologias digitais nas práticas investigativas. A análise histórica permitiu compreender como as transformações tecnológicas moldaram o comportamento humano e as dinâmicas sociais, criando novos desafios para o sistema de justiça. A introdução de ferramentas digitais, como algoritmos e inteligência artificial, trouxe à tona a necessidade de uma reflexão crítica sobre a substituição da análise humana pela automação, destacando a importância da interpretação e do discernimento humano nas investigações.

O segundo capítulo concentrou-se nos métodos investigativos utilizados pelas autoridades policiais, especialmente em operações de grande escala. Foram examinados os critérios que levam à deflagração dessas operações e a eficácia dos métodos empregados. A discussão sobre a coleta de dados de aparelhos telefônicos e o uso de *spywares* evidenciou a tensão entre segurança e privacidade, ressaltando a necessidade de regulamentação para proteger os direitos dos indivíduos. A análise das implicações legais dessas práticas foi fundamental para entender os limites éticos e jurídicos que devem ser respeitados.

No terceiro capítulo, a dissertação abordou a Lei 12.965/2014, conhecida como Marco Civil da Internet, e sua aplicação na jurisprudência brasileira. A análise das decisões judiciais revelou os desafios enfrentados na interpretação da lei em relação ao acesso a dados armazenados eletronicamente. A pesquisa destacou a importância de um entendimento harmonioso entre a legislação e as práticas investigativas, enfatizando a necessidade de um equilíbrio entre a proteção da privacidade e a eficácia das investigações.

Trouxe à tona a discussão sobre os *standards* probatórios e a fundamentação judicial necessária para garantir a segurança jurídica no acesso, uso e gestão de dados armazenados. A análise crítica das normas existentes e das lacunas na legislação atual evidenciou no quarto capítulo a urgência de se estabelecer um marco regulatório que

defina claramente os critérios e procedimentos para o acesso a dados eletrônicos. As sugestões apresentadas neste capítulo foram fundamentais para a construção de um modelo que respeite os direitos fundamentais dos indivíduos, ao mesmo tempo em que permita a atuação eficaz das autoridades investigativas.

A importância de criar uma legislação específica para estipular *standards* probatórios para o acesso a dados estáticos armazenados em dispositivos eletrônicos não pode ser subestimada. A ausência de uma regulamentação clara pode levar a abusos e violações de direitos, comprometendo a confiança da sociedade nas instituições de justiça. A proposta de um marco legal que estabeleça critérios objetivos para o acesso a dados, incluindo a necessidade de autorização judicial e a definição de situações excepcionais, é essencial para garantir a proteção dos direitos dos cidadãos.

Além disso, a criação de uma legislação robusta deve incluir diretrizes sobre a transparência e a prestação de contas das autoridades que realizam investigações. A sociedade deve ser informada sobre os métodos utilizados e as justificativas para o acesso a dados, promovendo um ambiente de confiança e respeito aos direitos individuais. A regulamentação deve também prever mecanismos de controle e supervisão, assegurando que as práticas investigativas sejam realizadas dentro dos limites da legalidade.

A pesquisa também destacou a necessidade de capacitação e formação contínua para os profissionais envolvidos nas investigações. A complexidade das tecnologias digitais exige que os operadores do direito estejam atualizados sobre as inovações e suas implicações legais. A formação adequada é crucial para garantir que as investigações sejam conduzidas de maneira ética e responsável, respeitando os direitos dos indivíduos e a integridade do processo judicial.

Outro ponto relevante abordado na dissertação foi a importância da colaboração entre diferentes setores, incluindo o judiciário, o legislativo e as agências de segurança pública, pois a construção de um diálogo interinstitucional é fundamental para o desenvolvimento de políticas públicas que atendam às demandas da sociedade contemporânea, garantindo a segurança pública sem comprometer os direitos fundamentais.

Por fim, a dissertação conclui que a correlação entre tecnologia e direito é um campo em constante evolução, que requer atenção e adaptação contínuas. A criação de uma legislação que estabeleça *standards* probatórios claros e objetivos para o acesso a dados armazenados em dispositivos eletrônicos é uma necessidade premente. Essa legislação deve ser construída com base em princípios de proteção dos direitos humanos,

transparência e responsabilidade, assegurando que as investigações criminais sejam realizadas de forma justa e equitativa.

REFERÊNCIAS

ABREU, Jacqueline de Souza. **Guarda obrigatória de registros de telecomunicações no Brasil: Sobre as origens da retenção de dados e as perspectivas para direitos fundamentais**. P. 2. *In*: Disponível em: https://lavits.org/wp-content/uploads/2017/08/P5_De_Souza_Abreu.pdf

ALMEIDA, Virgílio Augusto Fernandes. **Recomendações para o avanço da inteligência artificial no Brasil**. GT-IA da Academia Brasileira de Ciências. Rio de Janeiro-RJ. 2023. Disponível em: https://www.abc.org.br/wp-content/uploads/2023/11/recomendacoes-para-o-avanco-da-inteligencia-artificial-no-brasil-abc-novembro-2023-GT-IA.pdf

ARNAUD, Raraela Rocha; TARGINO, Giliard Cruz; ESTRELA, William Marques. **Mutação constitucional: A atuação do poder constituinte difuso no Brasil**. Revista Interdisciplinar e do Meio Ambiente-ISSN 2674-693X -v.1, n.1, 2019, e41. P. 4). Disponível em: https://caroa.org.br/revista/index.php/rima/article/view/59/21

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. **A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência**. Revista de Investigações Constitucionais 4, no. 3 (2019): 167-200. p. 15. Disponível em: https://doi.org/10.5380/rinc.v4i3.51295

ÁVILA, Gustavo Noronha de; SILVA, Luís Gustavo Candido. **O fenômeno da pescaria probatória e os mandados de busca e apreensão genéricos nas operações de combate à corrupção da tutela (in)efetiva dos direitos personalíssimos à intimidade e ao sigilo profissional do contador**. Arquivo Jurídico – Revista Jurídica Eletrônica da UFPIISBN 2317-918X – V. 10, n. 2, jul/dez 2023. Disponível em: https://revistas.ufpi.br/index.php/raj/article/view/13803/8558

BADARÓ, Gustavo Henrique. **Processo Penal**. 9. ed. rev., atual. e ampl. -- São Paulo : Thomson Reuters Brasil, 2021.

BELANDI, Caio. **161,6 milhões de pessoas com 10 anos ou mais de idade utilizaram a Internet no país, em 2022**. Agência IBGE Notícias. 09.11.2023. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38307-161-6-milhoes-de-pessoas-com-10-anos-ou-mais-de-idade-utilizaram-a-internet-no-pais-em-2022#:~:text=Destaques,62%2C1%25%20em%202022.

BENDLIN, Rafaela Witt.; WITT, Cleonice. **A interseção entre proteção de dados e direito à privacidade no contexto digital**. CONTRIBUCIONES A LAS CIENCIAS SOCIALES, [S. l.], v. 17, n. 7, p. e8250, 2024. DOI: 10.55905/revconv.17n.7-112. P. 1 e 2. Disponível em: https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/8250

BITTENCOURT, Cezar Roberto. **Tratado de Direito Penal: Parte Geral (arts. 1º a 120)**. 29. ed. – São Paulo: SaraivaJur, 2023. (v. 1) .

BOEING, Daniel Henrique Arruda; ROSA, Alexandre Morais da. **Ensinando um Robô a Julgar. Pragmática, discricionariedade, heurísticas e vieses no uso de aprendizado de máquina no Judiciário**. 1ª Ed. Florianópolis-SC: Emais Academia, 2020.

BORGES, Amanda Tavares; CARDOSO, Priscila Mara Garcia. **Segurança pública e organizações criminosas no Brasil: Uma análise das ferramentas de investigação utilizadas pela Polícia Civil do Estado de São Paulo**. Revista de Movimentos Sociais e Conflitos | e-ISSN: 2525-9830 | Encontro Virtual | v. 6 | n. 2 | p. 42 - 60 | Jul/Dez. 2020.

BORGES, Clara Maria Roman. **A genealogy of the critical discourses on the authoritarianism of the Brazilian Criminal Procedure Code**. Sequência (Florianópolis) [Internet]. 2021;42(87):e63139. Disponível em: https://doi.org/10.5007/2177-7055.2021.e63139

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL. Superior Tribunal de Justiça**. AgRg no RMS 71.168-RJ (2023/0124057-3)**. Rel. Min. Laurita Vaz. Rel. P. Acórdão Min. Jesuíno Rissato (desembargador convocado). 6ª Turma, Brasília/DF, DJ 30.08.2023. Disponível em: https://scon.stj.jus.br/SCON/. Palavras-chave: "registro de conexão"; "Lei n. 12.965/2014"; "histórico de navegação".

BRASIL. Superior Tribunal de Justiça. ***Habeas Corpus* 444.024-PR (2018/0078245-6)**. Rel. Min. Sebastião Reis Jr.. Rel. P. Acórdão Min. Rogerio Schietti Cruz. 6ª Turma, Brasília/DF, DJ 02.08.2019. Disponível em: https://scon.stj.jus.br/SCON/. Palavras-chave: "mídias"; "Lei n. 12.965/2014"; "acesso"; "informações"; "dados estáticos".

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. **Lei de Interceptação Telefônica**. Lei Federal 9.296/96, de 24.07.1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm

BRASIL. **Marco Civil da Internet (2014)**. Lei 12.965 de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. Supremo Tribunal Federal. **ARE 1.042.075/RJ**. Rel. Ministro Gilmar Mendes. Tribunal Pleno, Brasília/DF. Em julgamento.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 418.416/SC**. Rel. Ministro Sepúlveda Pertence. Tribunal Pleno, Brasília/DF, DJ 19.12.2006.

BRASIL. Supremo Tribunal Federal. ***Habeas Corpus* 91.867/PA**. Rel. Ministro Gilmar Mendes. 2ª Turma, Brasília/DF, DJe 20/09/2012.

BRASIL. Supremo Tribunal Federal. ***Habeas Corpus* 78.250.** Rel. Ministro Maurício Corrêa. 2ª Turma, Brasília/DF, DJe 26.02.1999.

BRASIL. Tribunal de Justiça do Distrito Federal. **Mandado de Segurança n. 0714619-24.2020.8.07.000.** Rel. Desembargador João Timóteo de Oliveira, Câmara Criminal, Brasília/DF, DJe 17/12/2020.

CARDOSO, Daniel Keiny; RODRIGUES, Paulo Alexandre. **O emprego do operador de operações especiais em conjunto com o agente de inteligência**. Brazilian Journal of Development, *[S. l.]*, v. 9, n. 6, p. 20481–20494, 2023. DOI: 10.34117/bjdv9n6-114. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/60865

Cartilha de Segurança para Internet, versão 4.0. CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf

DUARTE, Andreia Filipa Santos. **O *malware* como meio de obtenção de prova em processo penal**. Repositório científico da UC. Coimbra, 2022. Disponível em: https://hdl.handle.net/10316/103589

FACHIN, Luiz Edson; ESTEVES, Fabio Francisco. **Processo Penal, Tecnologia e Democracia**. Org.: MADEIRA, Guilherme; BADARÓ, Gustavo; SCHIETTI, Rogerio. Código de Processo Penal: Estudos Comemorativos aos 80 anos de Vigência: Vol. 1. São Paulo: Thomson Reuters Brasil, 2021.

FERNANDES, Maíra. QUITO, Carina. **Riscos do uso de *softwares* espiões em atividades de persecução criminal e de inteligência**. Conjur. 12.06.2024. Disponível em: https://www.conjur.com.br/2024-jun-12/riscos-do-uso-de-softwares-espioes-em-atividades-de-persecucao-criminal-e-de-inteligencia/

GRECO, Luís; GLEIZER, Orlandino. **A infiltração online no processo penal – Notícia sobre a experiência alemã**. Rev. Bras. de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, set.-dez. 2019.

GRECO, Luís. **Poder de julgar sem responsabilidade de julgador: A impossibilidade jurídica do juiz-robô**. São Paulo, SP: Marcial Pons, 2020.

GIACOMOLLI, Felipe. **Gerenciamento Tecnológico do Sistema de Justiça Penal: As novas tecnologias no âmbito do policiamento, da investigação e da decisão**. 1. Ed. Rio de Janeiro: Marcial Pons. 2023.

GUZZO, Matheus Muniz. **A Violação do Princípio da Legalidade pelas Normas Penais em Branco: uma Visão Sistematizada do Estatuto do Desarmamento**. Revista do Ministério Público do Rio de Janeiro nº 67, jan./mar. 2018. P. 185. Disponível em: https://www.mprj.mp.br/documents/20184/1245317/Matheus_Muniz_Guzzo.pdf

HENRIQUES, Marco Ribeiro. **Ações encobertas, para fins de investigação criminal. A dicotomia entre agente infiltrado e agente provocador**. Revista Jurídica UNIGRAN. Dourados, MS | v. 18 | n. 34 | Jan./Jun.2016. Disponível em: https://www.researchgate.net/profile/Marco-Ribeiro-Henriques/publication/309618668_Acoes_encobertas_para_fins_de_investigacao_criminal_A_dicotomia_entre_Agente_Infiltrado_e_Agente_Provocador/links/581a1d9708ae3

c82664c173f/Acoes-encobertas-para-fins-de-investigacao-criminal-A-dicotomia-entre-Agente-Infiltrado-e-Agente-Provocador.pdf

HUREL, Louise Marie; FRANCISCO, Pedro Augusto P. TELES, Daisy. **Pegasus, a ponta do iceberg da fragilidade no controle de inteligência e uso de tecnologias de vigilância**. El País. 02.08.2021. Disponível em: https://brasil.elpais.com/opiniao/2021-08-02/pegasus-a-ponta-do-iceberg-da-fragilidade-no-controle-de-atividades-de-inteligencia-e-uso-de-tecnologias-de-vigilancia.html

ISRAEL, Carolina Batista. **Território, jurisdição e ciberespaço: entre os contornos westfalianos e a qualidade transfronteiriça da Internet.** Geousp – Espaço e Tempo (On-line), v. 24, n. 1, p. 69-82, abr. 2020. ISSN 2179-0892. Disponível em: https://doi.org/10.11606/issn.2179-0892.geousp.2020.161521

JARDIM, Afrânio Silva; AMORIM, Pierre Souto Maior Coutinho. **Primeiras Impressões Sobre a Lei n. 13.964/19, Aspectos Processuais**. Org.: MADEIRA, Guilherme; BADARÓ, Gustavo; SCHIETTI, Rogerio. Código de Processo Penal: Estudos Comemorativos aos 80 anos de Vigência: Vol. 1. São Paulo: Thomson Reuters Brasil, 2021.

LIU, Chuncheng. **Who supports expanding surveillance? Exploring public opinion of Chinese social credit systems**. International Sociology, 37(3), 391-412. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/542

LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. 2.ed., rev. e atual. 2 São Paulo: Editora JusPodivm. 2024.

LUCCHESI, Guilherme Brenner; VIDA, Lucas Gandolfi. **Perspectivas quanto à lavagem de provas na colaboração premiada: proposta para controle de abuso processual**. Revista Brasileira de Direito Processual Penal, *[S. l.]*, v. 7, n. 3. 2021. Disponível em: https://doi.org/10.22197/rbdpp.v7i3.542

MAIA, Tiago Dias; PAULINO, Galtiênio da Cruz. **A quebra de sigilo de dados baseada em coordenadas geográficas e o princípio da proporcionalidade**. Escola Superior do Ministério Público da União. P. 778. Disponível em: https://escola.mpu.mp.br/publicacoes/obras-avulsas/e-books-esmpu/direitos-fundamentais-em-processo-2013-estudos-em-comemoracao-aos-20-anos-da-escola-superior-do-ministerio-publico-da-uniao/44_a-quebra-de-sigilo-de-dados.pdf

MARCHI, Késsia Rita da Costa; VALENTIM, Marta Lígia Pomim; BOTEGA, Leonardo Castro. **A Filosofia da informação e a Sociedade da informação e do conhecimento: reflexões diante do progresso tecnológico**. InCID: Revista de Ciência da Informação e Documentação, Ribeirão Preto, Brasil, v. 12, n. 2, p. 32–51, 2021. DOI: 10.11606/issn.2178-2075.v12i2p32-51. Disponível em: https://www.revistas.usp.br/incid/article/view/183305.

MATIDA, Janaina; VIEIRA, Antonio. P**ara além do BARD: uma crítica à crescente adoção do *standard* de prova "para além de toda a dúvida razoável" no processo penal brasileiro**. Revista Brasileira de Ciências Criminais, v. 156. 2019.

MENDES, Gilmar F.; BRANCO, Paulo G. G. **Curso de Direito Constitucional**. Saraiva, 2013. E-book.

MENDES, Gilmar Ferreira.; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 12 ed. São Paulo: Saraiva, 2015.

MONTEIRO, Júlia Iunes; MARRAFON, Marco Aurélio. **Legitimidade democrática na governança algorítmica: Primeiros parâmetros para sua aplicação na regulação e no desenvolvimento da inteligência artificial e de políticas baseadas em dados**. Revista Direitos Fundamentais & Democracia V. 29, N. I. jan./abril, 2024. P. 8 e 9. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2747/805

MOREIRA, Leandro Mara. **Busca domiciliar: legislação, jurisprudência antidogmática e ativismo judicial**. Revista Processus de Estudos de Gestão, Jurídicos e Financeiros,Ano 15, Vol. XV, n.48, jan.-jul., 2024. Disponível em: https://zenodo.org/records/10815702

NETO, Mario Azambuja. **Investigação criminal pelo Ministério Público: Para além da questão da (im)possibilidade**. Rev. SJRJ, Rio de Janeiro, v. 17, n. 29, p. 151-174, dez. 2010. Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/74980/investigacao_criminal_pelo_azambuja.pdf

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. ISSN 1984-7858. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130.

NYBO, Erik Fontenele. **Eu, Robô: como dados pessoais podem ser utilizados pela inteligência artificial e os impactos que esse uso pode gerar**. Coordenação: PALHARES, Felipe. Estudos sobre Privacidade e Proteção de Dados. São Paulo: Thomson Reuters Brasil. 2021.

OLIVEIRA, Lurã Azevedo de; MEDINA, Lucas Arieh Bezerra. **A cadeia de custódia das provas colhidas em aparelhos móveis de gravação**. Boletim IBCCRIM, [S. l.], v. 31, n. 364, p. 16–19, 2024. P. 18. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1584

PEREIRA, Fábio Luiz Barboza. **Preocupações sobre a proteção de dados pessoais em veículos autônomos**. Coordenação: PALHARES, Felipe. Estudos sobre Privacidade e Proteção de Dados. São Paulo: Thomson Reuters Brasil. 2021.

PINHEIRO, Juliana Ferreira Soares. **Contornos da cadeia de custódia no âmbito da interceptação telefônica**. 2021. 51 f. — Universidade de Brasília, Brasília, 2021. Disponível em: https://bdm.unb.br/handle/10483/29806

PINHEIRO, Victor Sales; BONNA, Alexandre Pereira. **Sociedade da informação e direito à privacidade no Marco Civil da Internet: fundamentação filosófica do Estado de Direito**. Revista de Direitos e Garantias Fundamentais, *[S. l.]*, v. 21, n. 3, p.

365–394, 2020. DOI: 10.18759/rdgf.v21i3.1555. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1555.

PRADO, Luis Fernando. **Algoritmos e decisões automatizadas: Buscando conformidade com a LGPD**. Coordenação: PALHARES, Felipe. Estudos sobre Privacidade e Proteção de Dados. São Paulo: Thomson Reuters Brasil. 2021.

RANGEL, Paulo. **Breves considerações sobre a Lei 9.296/96 - Interceptação telefônica**. Revista do Ministério Público, Rio de Janeiro, RJ, (6), 1997.

RIBEIRO, Gustavo A. M.; CORDEIRO, Pedro Ivo R. V.; FUMACH, Débora M. **O *malware* como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro**. Revista Brasileira de Direito Processual Penal, vol. 8, n. 3, p. 1463-1500, set./dez. 2022. Disponível em: https://doi.org/10.22197/rbdpp.v8i3.723

ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico de acordo com a teoria dos jogos e MCDA-C**. 1. Ed. Florianópolis [SC]: Emais, 2021.

SANTOS, Célio Jacinto dos. **A gênese das grandes operações investigativas da polícia federal**. Revista Brasileira de Ciências Policiais. Brasília, v. 8, n. 2, p. 9-66, jul/dez 2017. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/526/309

SARLET, Ingo. **A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I**. Consultor Jurídico. 11.03.2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental/

SCALCON, Raquel; FERREIRA, André da Rocha. **O problema da quebra coletiva de sigilo de dados pessoais contra pessoas indeterminadas**. Boletim IBCCRIM 31, no. 370 (2023): 18-20.

SCHEUERMANN, Gabriela Felden. **Dados pessoais como um direito fundamental autônomo a partir da Emenda Constitucional nº 115/2022**. Revista da Defensoria Pública do Estado do Rio Grande do Sul, Porto Alegre, v. 2, n. 33, p. 253–274, 2023. Disponível em: https://revistadpers.emnuvens.com.br/defensoria/article/view/600.

SILVA, Virgílio Afonso da. **O Proporcional e o Razoável**. Revista dos Tribunais 798 (2002): 23-50. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/97313

SILVER, David. *et al*. **AlphaZero: Shedding new light on chess, shogi, and Go**. Disponível em: https://deepmind.google/discover/blog/alphazero-shedding-new-light-on-chess-shogi-and-go/

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, Brasília, Brasil, v. 12, n. 5, p. 49–76, 2021. Disponível em: https://doi.org/10.31412/rbcp.v12i5.840.

SMANIO, Gianluca Martins. **Vigilância policial em meio digital: Entre o garantismo e a eficiência**. Curitiba: Juruá, 2022.

STRECK, Lenio Luiz; RAATZ, Igor. **O Dever de Fundamentação das Decisões Judiciais sob o Olhar da Crítica Hermenêutica Do Direito**. Revista Opinião Jurídica, vol. 15, núm. 20, julio, 2017, pp. 160-179. Centro Universitário Christus Ceará, Brasil. Disponível em: https://www.redalyc.org/articulo.oa?id=633868963015

TAVARES, João Paulo Lordelo Guimarães. **O regime jurídico das provas digitais no direito brasileiro.** Revista de Processo. vol. 316. ano 46. p. 373-387.São Paulo: Ed. RT, junho 2021. Disponível em: https://civilprocedurereview.com/revista/article/view/217

VASCONCELLOS, Vinícius Gomes de. ***Standard* probatório para condenação e dúvida razoável no processo penal: análise das possíveis contribuições ao ordenamento brasileiro**. Revista Direito GV, v. 16, n. 2, 2020. P. 6. Disponível em: https://www.scielo.br/j/rdgv/a/9wZMTLkctLvR5knhRqXxZ6B/?lang=pt

VAZ, Denise Provasi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório**. 2012. Tese (Doutorado em Direito Processual) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/pt-br.php

VIANNA, Tulio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de direito penal informático**. Repositório UFMG. Dissertação de Mestrado. 2001. P. 85 e 86. Disponível em: http://hdl.handle.net/1843/BUOS-96MPWG

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância. A luta por um futuro humano na nova fronteira do poder**. Tradução de George Schlesinger. 1. ed. - Rio de Janeiro: Intrínseca, 2020. P. 20.