UNIVERSIDADE NOVE DE JULHO

PÓS-GRADUAÇÃO *STRICTO SENSU*

PROGRAMA DE MESTRADO EM DIREITO

NATALIA CEZARIO CARVALHO

PROVAS DIGITAIS: UM NOVO PANORAMA JURÍDICO-SOCIAL

SÃO PAULO

2024

UNIVERSIDADE NOVE DE JULHO

PÓS-GRADUAÇÃO *STRICTO SENSU*

PROGRAMA DE MESTRADO EM DIREITO

NATALIA CEZARIO CARVALHO

PROVAS DIGITAIS: UM NOVO PANORAMA JURÍDICO-SOCIAL

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Direito da Universidade Nove de Julho – UNINOVE, como requisito parcial para obtenção do título de mestre em Direito.

Orientador: Prof. Dr. Rogério Schietti Cruz

SÃO PAULO

2024

Carvalho, Natalia Cezario.

Provas digitais: um novo panorama jurídico-social. / Natalia Cezario Carvalho. 2024.

208 f.

Dissertação (Mestrado) - Universidade Nove de Julho - UNINOVE, São Paulo, 2024.

Orientador (a): Prof. Dr. Rogerio Schietti Cruz.

1. Dados informáticos. 2. Sigilo de dados. 3. Investigação. 4. Processo penal.

NATALIA CEZARIO CARVALHO
PROVAS DIGITAIS: UM NOVO PANORAMA JURÍDICO-SOCIAL

Dissertação apresentada ao Programa de Pós-Graduação Stricto Sensu em Direito da Universidade Nove de Julho como parte das exigências para a obtenção do título de Mestre em Direito.

São Paulo, 10 de dezembro de 2024.

BANCA EXAMINADORA

Prof. Dr. Rogerio Schietti Machado Cruz
Orientador
UNINOVE

gov.br Documento assinado digitalmente
SAMANTHA RIBEIRO MEYER PFLUG MARQUES
Data: 06/01/2025 10:11:48-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Samantha Ribeiro Meyer
Examinadora Interna UNINOVE

Profa. Dra. Danyelle da Silva Galvão
Examinador Externo
IDP

Dedico este trabalho a todos os profissionais que enfrentam os desafios de adaptar a prática jurídica às novas tecnologias, buscando sempre a proteção dos direitos fundamentais e a realização de um processo justo e eficiente.

AGRADECIMENTOS

Em primeiro lugar, agradeço a todas as experiências e lições que a vida me proporcionou. Os obstáculos, conquistas e pessoas que cruzaram meu caminho contribuíram e me impulsionaram a seguir firme na busca dos meus sonhos.

A fé inabalável me sustentou em todos os momentos, dando forças para continuar mesmo diante dos maiores desafios, guiando meus passos e mantendo vivo o propósito de nunca desistir.

A minha avó, Norma, que me acolheu desde o primeiro momento e sempre acreditou em mim. Lembro-me como se fosse hoje como vibrou quando soube que iria cursar direito. Tenho certeza de que, se ainda estivesse neste plano, estaria muito alegre e comemorando mais essa conquista.

Aos meus pais, Antônio Carlos e Suzana, exemplos de garra. A minha madrasta, Rozi, que sempre esteve ao meu lado e me apoiou.

Ao meu marido, André, que esteve comigo em todos os momentos.

Ao desembargador do Tribunal de Justiça, Dr. Carlos Monnerat, que sempre possibilitou minha evolução pessoal e profissional, incentivando na evolução dos estudos e dando absoluto suporte nesta etapa acadêmica.

A todos os meus amigos que estiveram ao meu lado, especialmente Cris Fairbanks e Bruna Massaroto. Obrigada pela amizade e paciência ao longo dessa jornada.

Aos professores da pós-graduação, homenagem que faço na pessoa da professora Samantha Meyer que, desde o primeiro dia, trouxe ensinamentos que levarei para toda vida.

Ao meu orientador, professor Dr. Rogerio Schietti, pela confiança. Muito obrigada por todo conhecimento transmitido.

A banca examinadora, pela experiência, disponibilidade, sugestões e correções para o trabalho.

Que este marco seja apenas o início de novas jornadas e realizações.

“A massa mantém a marca, a marca mantém a mídia e a mídia controla a massa”.

(George Orwell)

RESUMO

O presente trabalho analisa o contexto das provas digitais e suas implicações na investigação criminal. Inicia-se com o estudo da prova no processo penal e historicidade das leis que versam sobre o tema. Além disso, aborda a investigação de crimes em meios tecnológicos e os procedimentos para requisição dos dados atualmente utilizados, analisando a consecução de provas e a possibilidade de sua validação. Também analisa como tais disposições encontram óbice ou amparo na legislação atual, com debate sobre os acordos de cooperação internacional e eventuais conflitos diante da soberania nacional, à luz dos princípios constitucionais. O trabalho se desenvolve pelo percurso metodológico lógico-sistemático, colacionando jurisprudência e doutrina. Ao final, foram traçadas conclusões acerca das indagações quanto aos dados informáticos e também sobre a necessidade de regularização sobre o tema.

Palavras-chave: Dados informáticos. Sigilo de dados. Investigação. Processo Penal.

ABSTRACT

This work analyzes the context of digital evidence and its implications for criminal investigation. It begins with the study of the evidence in the criminal process and the historicity of the law about the topic. Furthermore, analyzes the investigation of crimes using technological procedures and how its works and the validation. Also studies about obstacles or support in current legislation, international cooperation agreements and possible conflicts with other nations. This work is developed through a logical-systematic methodological path, bringing court decisions and doctrine. In the end, conclusions about the questions of computer datas and the needed for regulatization.

Keywords: Computer data. Data confidentiality. Investigation. Criminal proceedings.

LISTA DE ABREVIATURAS

ACEL	Associação Nacional das Operadoras Celulares
Anatel	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
CF/88	Constituição Federal de 1988
CGI	Comitê Gestor da Internet
Coaf	Conselho de Controle de Atividades Financeiras
CPC	Código de Processo Civil
CPP	Código de Processo Penal
DOU	Diário Oficial da União
DPO	*Data Protection Officer*
GDPR	*General Data Protection Regulation*
IA	Inteligência Artificial
IBGC	Instituto Brasileiro de Governança Corporativa
IBGE	Instituto Brasileiro de Geografia e Estatística
INTELSAT	*International Telecommunications Satellite Organization*
IP	*Internet protocol*
LGDP	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
MLAT	*Mutual Legal Assistence Treaty*
MP	Ministério Público
RGPD	Regulamento Geral de Proteção de Dados Pessoais
RIPD	Relatório de Impacto à Proteção de Dados Pessoais
SEC	*Securities and Exchange Comission*
STF	Supremo Tribunal Federal
UIF	Unidade de Inteligência Financeira

USP	Universidade Federal de São Paulo
VPN	*Virtual Private Network*

SUMÁRIO

INTRODUÇÃO

A tecnologia rompeu com as referências tradicionais em diversos aspectos, evidenciando a mudança de paradigma que reverberou no direito material e processual penal.

Com o surgimento da *internet* e o âmbito virtual cada vez mais presente nas relações, inevitavelmente, os crimes também passaram a ser praticados no domínio digital.

Todo esse contexto mudou a maneira como os assuntos do cotidiano são vistos. Se antes os crimes ocorriam de determinada forma e a investigação era conduzida por meio da produção de provas num modelo analógico (dependendo de documentos físicos e comunicações presenciais), hoje é possível - e necessário - utilizar instrumentos tecnológicos na investigação, como câmeras, *smartphones* e acesso à *internet*, o que tenciona a necessidade de adaptação das técnicas de investigação para o ambiente virtual.

Nesse sentido, há um novo panorama jurídico-social que denota a necessidade de analisar o processo penal dentro desse viés e, consequentemente, as provas digitais, afinal, o local de crime que antes era um endereço postal, agora passa a ser identificado por meio de um *internet protocol* (IP).

Dessa forma, um ponto importante a ser analisado é a integração das esferas transnacionais, sendo imprescindível e premente tal adaptação, vez que a prova digital é dotada de grande volatidade, considerando os meios de armazenamento.

Com a *internet* e as novas tecnologias de informação tão enraizados na vida social, não existe mais a possibilidade de ignorar suas análises em quaisquer processos de investigação e todos os sistemas informáticos ali inseridos, afinal, é por meio disso que quase a totalidade das tarefas são realizadas atualmente, notadamente as empresariais.

Assim, esta produção tem o propósito de estudar o conteúdo e alcance da utilização da prova digital para a investigação criminal e, consequentemente, na ação penal, à luz dos princípios constitucionais, ordenamento jurídico pátrio e acordos de cooperação internacional.

Conforme a linha de pesquisa que visa a análise de estruturas do Direito Empresarial, serão examinadas as mudanças legislativas, assim como as estratégias jurídicas e organizacionais adotadas para esse fim. Da mesma forma, será avaliado de que forma a busca pela eficiência (com processos mais céleres) se harmoniza com a preservação dos direitos e liberdades individuais assegurados na Constituição Federal.

O objeto da investigação é a modernização do Direito Processual Penal sob a ótica da eficiência da justiça. Para tanto, trazer-se-á em cena o *corpus* do estudo e os movimentos que se farão presentes no processo de construção acerca da análise de tais dados e sua utilização no

processo penal, tecendo debates sobre o Direito Penal como *ultima ratio*, em razão do impacto nas liberdades individuais àqueles condenados nessa esfera, traçando um paralelo com as novas faces da criminalidade.

Por conseguinte, serão analisados os direitos essenciais relacionados ao processo penal, responsáveis por fundamentar o Estado de Direito, com a ideia de que eventuais excessos estatais podem ser contidos por um sistema penal que respeite a dignidade do investigado e/ou acusado, dentro dos critérios determinados pela Constituição da República, sem, no entanto, negligenciar a eficácia e a operacionalidade do sistema.

Ao examinar as organizações no contexto empresarial sob uma perspectiva econômica, a compreensão dos princípios constitucionais é enriquecida pela investigação da regulação em suas várias facetas, incluindo a regulação econômica, setorial e transnacional. Dessa forma, as bases do Direito Empresarial, Direito Penal e Processual Penal são fundamentais para a análise do poder financeiro e, nesse sentido, a regulação surge como elemento essencial nesse processo, principalmente diante da complexidade da sociedade contemporânea.

Assim, serão empreendidas buscas que extrapolarão o aspecto econômico, adentrando nos espaços de reflexões com vistas à privacidade, consenso, entre outros e, diante de tais inquietações, deparar-se-á com paradoxos e ambiguidades.

Nas estratégias a serem utilizadas no presente estudo, estarão mutuamente implicados o problema, o modo de colocá-lo e as ferramentas necessárias à pesquisa, com abordagem qualitativa, analisando o ordenamento jurídico, a doutrina e a jurisprudência, tendo como objetivos esboçados a compreensão, o alcance e os desafios relacionados à prova digital.

Como objetivo geral, o trabalho visa compreender e analisar o conteúdo das provas.

Como objetivos específicos, analisar o cenário neoconstitucional em relação à prova no processo penal, identificando o fornecimento de dados pelas empresas, sua utilização e como ocorre a proteção.

Logo, o problema de pesquisa do presente trabalho consiste em analisar a prova digital, de que forma os interesses individuais serão observados e a (des)necessidade de um diploma específico para tanto.

Com o fim de solucionar a problemática proposta e, tendo em vista o objetivo primário da pesquisa, os capítulos foram divididos didaticamente a fim de possibilitar que cada um, de forma lógica, forneça os elementos necessários para a conclusão que se seguirá.

Desse modo, no que concerne ao tônus teórico, será trazido à baila a teoria geral da prova, com propósito de demonstrar seu conceito, objetivos e importância para a condução do processo penal.

Em continuação, o segundo capítulo se ocupará dos impactos e desafios constitucionais diante da nova "era digital", analisando a *internet* e a colisão de direitos fundamentais, o sigilo de dados e sua proteção constitucional, o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD), a discussão sobre a LGPD Penal e a questão de política preventiva dentro do ambiente cibernético, tecendo considerações sobre a (im)possibilidade de monitoramento.

O terceiro capítulo, por sua vez, versa sobre a prova digital, analisando a investigação criminal no ambiente cibernético, suas origens, meios de obtenção de prova e custódia sob o enfoque da prova digital, analisando a forense digital em nuvem e passando pelas problemáticas da questão, como a *deep* e a *dark web*.

No quarto capítulo, será abordada a lavagem de dinheiro no contexto empresarial, com análise da autorregulação, governança corporativa e compliance e o mercado de apostas.

Por fim, o quinto capítulo abordará o fornecimento de dados por empresa transnacional, com análise da recente promulgação no Brasil da Convenção de Budapeste. Além disso, será analisada jurisprudência dos tribunais superiores, com vistas à identificação de ressonâncias ante aos anseios e transformações do tecido social.

O propósito é contribuir, somar esforços aos que têm se dedicado ao estudo da proteção de dados, investigações criminais e provas digitais.

Como cenário conclusivo, buscar-se-á observar todas as curvas e direções bibliográficas sobre a temática, visando agregar e gerar reflexão sobre os mecanismos de proteção frente às mazelas sociais impulsionadoras de leis mais efetivas.

1 A PROVA NO PROCESSO PENAL

1.1 CONCEITO E IMPORTÂNCIA DA PROVA

A prova apresenta diversas definições. No dicionário[1], é aquilo que "demonstra a veracidade de uma proposição, de um fato; comprovação".

Na etimologia da palavra, deriva do latim *probatio,* que significa verificação, confirmação, e o verbo provar deriva de *probare,* tendo como significado verificar, examinar, comprovar[2]. Nesse sentido, Edilson Mougenot tece as seguintes considerações:

> [...] para sermos absolutamente técnicos, devemos compreender que o termo "prova", no vocabulário jurídico brasileiro, é plurívoco, ou seja, dotado de significados diversos. No direito norte-americano, por exemplo, temos dois vocábulos distintos para a designação de coisas diversas: *evidence*, para indicar os meios de prova, e *proof*, para designar o resultado da atividade probatória no espírito do julgador. Assim, para que conceituemos *tecnicamente* o que seja prova no direito brasileiro, é necessário, portanto, num primeiro momento, descobrir as variadas significações do vocábulo em português, razão pela qual a prova pode ser entendida e conceituada como:
> a) a atividade realizada, em regra, pelas partes, com o fim de demonstrar a veracidade de suas alegações (p. ex., reconhecimento pessoal de "X" pela testemunha, observando o disposto no art. 226 do CPP);
> b) os meios ou instrumentos utilizados para a demonstração da verdade de uma afirmação ou existência de um fato (p. ex., o réu apresenta atestado médico – documento – comprovando que no dia Y, horário Z, foi submetido a exames);
> c) o resultado final da atividade probatória, ou seja, a certeza ou convicção que surge no espírito de seu destinatário.
> Daí por que falamos em "conceitos" de prova, e não em "conceito" (forma singular). Desse modo, prova será, com distinta acepção (conceito), dependendo do sentido que empreguemos ao vocábulo (itens acima)[3].

Assim, provar significa analisar a autenticidade de uma declaração sobre um acontecimento considerado real no mundo concreto. Para Guilherme de Souza Nucci[4], de forma subjetiva, prova é o resultado da ação de provar, ao passo que, num aspecto objetivo, será o meio de demonstração da verdade acerca de determinado fato, sendo o mecanismo mais apto para tanto.

Gustavo Henrique Badaró destaca:

---

[1] PROVA. *In:* **DICIO,** Dicionário Online de Português. Porto: 7Graus, 2024. Disponível em: https://www.dicio.com.br/prova. Acesso em: 10 abr. 2023.
[2] NUCCI, Guilherme de Souza. **Manual de Processo Penal** – Volume Único. 5. ed. Rio de Janeiro: Forense, 2024, p. 235.
[3] MOUGENOT, Edilson. **Curso de processo penal.** 14. ed. São Paulo: Saraiva Jur, 2024, p. 270.
[4] NUCCI, Guilherme de Souza. **Curso de direito processual penal**. 17. ed. Rio de Janeiro: Forense, 2020, p. 684.

> A palavra prova é polissêmica e seu estudo transcende ao Direito, envolvendo a Epistemologia, a Semiótica, a Psicologia e outras ciências afins.
> Em uma primeira aproximação, prova é tudo o que é apto a levar o conhecimento de alguma coisa a alguém. No entanto, esta é apenas uma das acepções do vocábulo prova. Tanto na linguagem comum quanto no campo do direito, a palavra prova possui outros significados. É comum indicar pelo menos três deles: (1) atividade probatória; (2) meio de prova; (3) resultado probatório.
> Prova como **atividade probatória** significa o conjunto de atos praticados para a verificação de um fato. É a atividade desenvolvida pelas partes e, subsidiariamente, pelo juiz, na reconstrução histórica dos fatos (por exemplo, a prova da alegação incumbe a quem a fizer – CPP, art. 156).
> A prova também pode ser considerada o **meio de prova**. Isto é, o instrumento por meio do qual se introduzem no processo os elementos probatórios. É nesse sentido que se fala em prova testemunhal, prova pericial etc.
> Finalmente, a prova pode ser identificada como o **resultado probatório**, isto é, o convencimento que os meios de prova geram no juiz e nas partes. Nesse sentido, por exemplo, o art. 312 do CPP se refere à "prova da existência do crime"[5].

No processo penal, portanto, o objetivo da parte é convencer o juiz, por meio de argumentos, de que sua interpretação dos acontecimentos é a válida, ou seja, que os fatos ocorreram na realidade da mesma forma como foram apresentados em sua petição. Ao se convencer dessa ideia, o juiz chega à certeza necessária para proferir sua decisão. Isso porque a descoberta da verdade é sempre relativa[6].

A prova, portanto, é o recurso utilizado pelos sujeitos processuais para comprovar os eventos relacionados à ação, ou seja, as afirmações apresentadas como base para a atuação do poder judiciário[7].

Dito por outras palavras, são as informações apresentadas no decorrer do procedimento, tanto pelas partes envolvidas quanto por aquelas determinadas pelo magistrado, com o intuito de persuadir o juiz a respeito dos acontecimentos que estão sendo analisados no momento[8].

O que se vê, portanto, é que não são exatamente os fatos que precisam ser validados através da evidência, mas as declarações apresentadas pelas partes, ou seja, suas alegações[9].

Nesse sentido, Aury Lopes Júnior ressalta que a prova é o meio de reconstrução de determinado acontecimento, permitindo ao julgador, portanto, a composição de sua convicção, a ser posteriormente expressa em decisão fundamentada, destacando, assim, o poder persuasivo da evidência[10]. Trata-se do que denomina de "ritual de cognição", sendo o processo penal:

---

[5] BADARÓ, Gustavo. **Processo Penal**.11. ed. São Paulo: Thomson Reuters Brasil, 2023, p. 380.
[6] NUCCI, Guilherme de Souza. **Manual de Processo Penal -** Volume Único. 5. ed. Rio de Janeiro: Forense, 2024, p. 235.
[7] MOUGENOT, Edilson. **Curso de processo penal.** 14. ed. São Paulo: Saraiva Jur, 2024, p. 270
[8] COSTA, Klaus Negri; ARAÚJO, Fábio Roque. **Processo Penal Didático**. 3. ed. Salvador: Juspodivm, 2020, p. 513.
[9] MOUGENOT, op. cit., p. 271.
[10] LOPES JÚNIOR, Aury. **Direito Processual Penal**. 21. edição. São Paulo: Saraiva, 2024, p. 391-392.

> [...] um instrumento de retrospecção, de reconstrução aproximativa de um determinado fato histórico. Como ritual, está destinado a instruir o julgador, a proporcionar o conhecimento do juiz por meio da reconstrução histórica de um fato. Nesse contexto, as provas são os meios através dos quais se fará essa reconstrução do fato passado (crime). O tema probatório é sempre a afirmação de um fato (passado), não sendo as normas jurídicas, como regra, tema de prova.
> Isso decorre do paradoxo temporal ínsito ao ritual judiciário: um juiz julgando no presente (hoje) um homem e seu fato ocorrido num passando distante (anteontem), com base na prova colhida num passado próximo (ontem) e projetando efeitos (pena) para o futuro (amanhã). Assim como o fato jamais será real, pois histórico, o homem que praticou o fato não é o mesmo que está em julgamento e, com certeza, não será o mesmo que cumprirá essa pena, e seu presente, no futuro, será um constante reviver o passado.
> O processo penal, inserido na complexidade do ritual judiciário, busca fazer uma reconstrução (aproximativa) de um fato passado. Através – essencialmente – das provas, o processo pretende criar condições para que o juiz exerça sua atividade recognitiva, a partir da qual se produzirá o convencimento externado na sentença[11].

A prova também é própria atividade probatória, visando a elaboração dos meios e ações executadas durante o procedimento com o objetivo de convencer o juiz sobre a veracidade de uma alegação acerca de um acontecimento relevante para a resolução do caso, sendo consequência direta do direito de ação, englobando não apenas o modo de apresentar argumentos ou solicitar a apresentação de provas, mas também a capacidade de influenciar na convicção do juiz; como resultado, marcado pela construção da certeza do julgador ao longo do processo em relação à presença (ou ausência) de determinada situação de fato; e, por último, como meio para que o juiz possa formar sua convicção[12].

Nesse sentido, Aury Lopes Júnior destaca que "é a prova que permite a atividade cognoscitiva do juiz em relação ao fato histórico (*story of the case*) narrado na peça acusatória"[13].

Segundo Edilson Mougenot:

> O processo é uma atividade racional, voltada à assunção de um objetivo, que é a aplicação do direito para obter a pacificação dos conflitos de interesses que surjam na sociedade. Nesse contexto, também a prova se pauta por regras e princípios organizados segundo critérios lógicos.
> Em primeiro lugar, é certo que a atividade probatória – ou seja, a série de atos realizados com a finalidade de desvendar os fatos tais como tenham esses efetivamente ocorrido – deve restringir-se aos fatos pertinentes à lide. A assertiva, óbvia em sua essência, é de fundamental importância: apenas os fatos que constituem, sob a incidência do ordenamento jurídico, as relações jurídicas relevantes para a resolução da lide é que deverão ser provados (princípio da economia processual).
> Em geral, a extensão da situação fática que deve ser demonstrada depende da atuação das partes. A acusação, ao imputar determinada conduta ao acusado, descreve uma série de fatos que em tese justificariam eventual condenação. O acusado, por sua vez,

[11] [11] LOPES JÚNIOR, Aury. **Direito Processual Penal**. 21. edição. São Paulo: Saraiva, 2024, p. 391-392.
[12] LIMA, Renato Brasileiro. **Manual de Processo Penal** – volume único. São Paulo: Juspodivm, 2022, p. 571-572.
[13] LOPES JÚNIOR, op. cit., p. 392.

> alegará fatos em sua defesa que de alguma forma contrariem a pretensão punitiva. São as partes, portanto, que definem essencialmente os fatos que deverão ser objeto de prova e a quem caberá, primordialmente, a gestão da prova, restando ao juiz, eventualmente, apenas complementar o rol de provas a produzir, utilizando-se de seu poder instrutório, o que determinará somente com a finalidade de fazer respeitar o princípio da verdade real [...][14].

Fato é que a prova será o meio pelo qual o juiz consegue atingir (certo) grau de verdade. Isso porque o conhecimento absoluto é algo que não pode ser atingido. O que se tem, portanto, é que a verdade obtida dentro de um processo penal é o alto nível de certeza de que determinada afirmação é correta, pois os eventos aconteceram como as evidências indicam[15].

Eugênio Paccelli faz alusão ao *mito e o dogma da verdade real* que, por muito tempo, disseminou a conduta inquisitiva como formalidade que deveria ser seguida estreme de dúvidas, de tal sorte que a busca por essa verdade fez com que a necessidade de sua obtenção como meta principal dentro do âmbito do processo penal não observasse quaisquer direitos e garantias – que, de todo modo, nem sequer estavam legalmente previstos. Nesse sentido, havia, sobremaneira, "a incumbência de legitimar eventuais desvios das autoridades públicas, além de justificar a ampla iniciativa probatória reservada ao juiz em nosso processo penal"[16].

Dessa forma, havia uma atuação judicial de modo supletivo à acusação, o que, atualmente, diante das garantias conferidas pela Constituição Federal de 1988 (CF/88) (especialmente contraditório e ampla defesa que traz a paridade de armas e imparcialidade no julgamento), já não é mais possível[17].

Fato é que toda verdade judicial é, portanto, uma "verdade meramente processual", pois será um axioma que emerge de uma reinterpretação. Segundo Gustavo Henrique Badaró:

> [...] a verdade é muito importante para o processo. Mas não é tudo. É preciso entender que *retirar a verdade do trono em que reinava absoluta no processo não significa desterrá-la*. Se a verdade não é centro do processo penal, não há como negar, por outro lado, que a verdade exerce um papel importante no processo, sendo o seu acertamento um dos seus escopos institucionais. Não se trata, portanto, de eliminá-la, mas de deslocá-la do lugar de centralidade, até então ocupado, para um ponto diverso, o que não significa secundário ou de pouca relevância[18].

Por outro lado, não se pode perder de vista que, diferentemente de outras áreas do direito, o processo penal é essencial para a aplicação efetiva do Direito Penal. Isso se deve ao

---

[14] MOUGENOT, Edilson. **Curso de processo penal**. 14. ed. São Paulo: Saraiva Jur, 2024, p. 271.
[15] BADARÓ, Gustavo. **Processo Penal**.11. ed., São Paulo: Thomson Reuters Brasil, 2023, p.375.
[16] PACELLI, Eugênio. **Curso de processo penal**. 28. edição. Lumen Juris: Rio de Janeiro, 2024, p. 284-286.
[17] PACELLI, loc. cit.
[18] BADARÓ, Gustavo Henrique. **Epistemologia Judiciária e Prova Penal**. 2. ed., São Paulo: Thomson Reuters, 2023, p. 133.

fato de que, enquanto no Direito Civil é possível a composição de bens sem a necessidade de atuação processual (por meio da jurisdição), no âmbito penal essa não é uma opção viável, vez que o bem jurídico em questão (a liberdade do indivíduo) não é passível de negociação. Assim, mesmo as formas alternativas de resolução de conflitos, que não exigem a produção de prova, seguem rígidos critérios de compensação, resultando em benefício consubstanciado em punição menos severa.

Nesse sentido, Aury Lopes Júnior ressalta ser "[...] um erro fazer transmissões mecânicas das categorias do processo civil para o processo penal, desconsiderando a especificidade do objeto do processo penal e o complexo ritual de exercício de poder estabelecido (absolutamente diferente do processo civil)"[19].

Segundo Eugênio Paccelli:

> Enquanto o processo civil aceita uma certeza obtida pela simples ausência de impugnação dos fatos articulados na inicial (art. 341, CPC/2015), sem prejuízo da iniciativa probatória que se confere ao julgador, no processo penal não se admite tal modalidade de certeza (frequentemente chamada de verdade formal, porque decorrente de uma presunção legal), exigindo-se a materialização da prova. Então, ainda que não impugnados os fatos imputados ao réu, ou mesmo confessados, compete à acusação a produção de provas da existência do fato e da respectiva autoria, falando-se, por isso, em uma verdade material[20].

Acerca da verdade a ser perseguida, Renato Brasileiro, em análise à historicidade do tema, destaca que:

> [...] no âmbito processual penal, estando em discussão a liberdade de locomoção do acusado, direito indisponível, o magistrado seria dotado de amplos poderes instrutórios, podendo determinar a produção de provas *ex officio*, sempre na busca da verdade material. Dizia-se então que, no processo penal, vigorava o princípio da verdade material, também conhecido como princípio da verdade substancial ou real. A descoberta da verdade, obtida a qualquer preço, era a premissa indispensável para a realização da pretensão punitiva do Estado. Essa busca da verdade material era, assim, utilizada como justificativa para a prática de arbitrariedades e violações de direitos, transformando-se, assim, num valor mais precioso do que a própria proteção da liberdade individual. A crença de que a verdade podia ser alcançada pelo Estado tornou a sua perseguição o fim precípuo do processo criminal. Diante disso, em nome da verdade, tudo era válido, restando justificados abusos e arbitrariedades por parte das autoridades responsáveis pela persecução penal, bem como a ampla iniciativa probatória concedida ao juiz, o que acabava por comprometer sua imparcialidade.
> Atualmente, essa dicotomia entre verdade formal e material deixou de existir. Já não há mais espaço para a dicotomia entre *verdade formal*, típica do processo civil, e *verdade material*, própria do processo penal.

[19] LOPES JÚNIOR, Aury. **Direito Processual Penal**. 21. edição. São Paulo: Saraiva, 2024, p. 398.
[20] PACELLI, Eugênio. **Curso de processo penal**. São Paulo: Atlas, 2017, p. 344.

> [...] essa busca da verdade no processo penal está sujeita a algumas restrições. Com efeito, é a própria Constituição Federal que diz que são inadmissíveis, no processo, as provas obtidas por meios ilícitos (art. 5º, LVI) [...][21].

Ainda sobre a prova, explica Manuel Valente que:

> [...] prova real não significa verdade real, pois são dimensões materiais dogmáticas jurídicas distintas, sendo que jamais se pode afirmar que num processo de produção de um fato passado se possa alcançar a verdade real. A verdade real não existe num processo-crime. No mundo físico a verdade esgota-se em cada milésimo de segundo e jamais pode ser reposta ou reedificada por meio de um processo reconstrutivo. São dimensões materiais dogmáticas distintas, sendo que em processo-crime, enquanto processo jurídico de convencimento e entendimento da prova, não existe verdade real, mas verdade processual[22].

Mas, como ressalva Aury Lopes Júnior, não basta ao juiz decidir porque assim quer - bastando sua convicção -, sendo "imprescindível que a essa dimensão se unam as regras do devido processo penal, da produção da prova válida, robusta e qualificada (qualidade epistêmica) para a construção racional da decisão"[23]. E, dessa forma, acrescenta que:

> [...] assumindo que existe uma esfera de subjetividade, precisamos então da outra dimensão: da construção racional e juridicamente válida da decisão. O ato decisório precisar estar amparado por argumentos cognoscitivos seguros, lógicos e válidos, construídos em cima de uma prova juridicamente válida e em contraditório, com enfrentamento das provas que refutam a hipótese tomada como verdadeira para a construção da decisão. É preciso que a decisão encontre abrigo no processo racional de sua construção, que não seja fruto do autoritarismo da mera vontade (decido assim porque eu quero), que seja demonstrável o caminho percorrido, ainda que se possa, obviamente, dela divergir (igualmente com argumentos racionais para uma refutação fundamentada).
> [...]
> Em suma, o processo penal tem uma finalidade retrospectiva, em que, através das provas, pretende-se criar condições para a atividade recognitiva do juiz acerca de um fato passado, sendo que o saber decorrente do conhecimento desse fato legitimará o poder contido na sentença[24].

Assim, a busca pela verdade não representa o objetivo final do processo penal, mas sim um recurso para garantir a aplicação adequada da legislação penal[25].

Em suma, a finalidade da prova é influenciar o juiz de modo a permitir que ele tome suas decisões tendo como supedâneo um certo grau de certeza. O intuito é formar seu

---

[21] LIMA, Renato Brasileiro. **Manual de Processo Penal** – volume único. São Paulo: Juspodivm, 2022, p. 68-69.
[22] VALENTE, Manuel Monteiro Guedes. **Cadeia de Custódia da Prova**. 4. ed. Coimbra: Almedina, 2023, p. 23.
[23] LOPES JÚNIOR, Aury. **Direito Processual Penal**. 21. edição. São Paulo: Saraiva, 2024, p. 395.
[24] Ibid., p. 396.
[25] BADARÓ, Gustavo. **Processo Penal**.11. ed., São Paulo: Thomson Reuters Brasil, 2023, p.379.

convencimento sobre um fato específico que aconteceu no passado e que agora está sendo analisado. Mas, de todo modo, a verdade *real* não será obtida.

Nos termos do artigo 155 do Código de Processo Penal (CPP), o juiz "formará sua convicção pela livre apreciação da prova produzida em contraditório", o que denota que o estudo da prova e suas consequências é de extrema relevância, vez que, após o devido processo legal, poderá haver sentença condenatória ou absolutória.

De todo modo, aqui se faz necessário um recorte metodológico, haja vista que não é objeto deste estudo a digressão conceitual acerca da busca da verdade real – daí porque tratado aqui de modo perfunctório, apenas para melhor entendimento quanto ao objetivo da prova.

No mais, sob qualquer viés que se analise tal tema, hoje é essencial garantir às partes todos os meios necessários para apresentar as provas, sob risco de limitar a defesa. Além disso, sua busca sempre deverá ser regida pelo respeito aos direitos e garantias fundamentais, pois a legitimação está condicionada à validade daquela prova produzida, sendo inadmissível que sejam obtidas por meios ilícitos (conforme art. 5º, inciso LVI da CF/88).

O Estado não pode, em nome da punição de alguém – aliado ao clamor público que é cada vez mais evidenciado por meio das redes sociais e a velocidade com a qual as notícias são propagadas - se desvincular da necessária observância às regras.

Em outras palavras, as garantias individuais estabelecidas no art. 5º da CF/88, além dos documentos internacionais afirmativos de direitos (como o Pacto de San José da Costa Rica), faz com que aquele modelo precipuamente instituído no CPP de 1941 (com um viés inquisitorial), seja comensurado com base nessas novas estruturas.

Imperioso também destacar as diversas classificações acerca da prova, a depender da doutrina analisada, existindo alguns critérios norteadores. Dessa forma, pode ser: a) *testemunhal*, que se refere à expressão verbal individual, sendo categoria de prova oral (mais ampla), englobando os depoimentos do perito e do assistente técnico, além das declarações eventuais da vítima, em clara manifestação de um indivíduo, não importando se é considerado tecnicamente testemunha ou não; b) *documental*, que é uma forma escrita que contém a afirmação da presença (ou ausência) de uma ação ou de um evento, resumindo visualmente a expressão de ideias, como, por exemplo, um acordo; e c) *material*, que trata-se da comprovação de um determinado acontecimento, evidenciando sua existência concreta, como o corpo de prova, por exemplo. Em resumo, representa qualquer elemento que comprove a ocorrência do fato[26].

[26] LIMA, Renato Brasileiro. **Manual de Processo Penal** – volume único. São Paulo: Juspodivm, 2022, p. 574.

Acerca da finalidade da prova, segundo Pacelli, tem o objeto de reconstruir os "fatos investigados no processo, buscando a maior coincidência possível com a realidade histórica, isto é, com a verdade dos fatos, tal como efetivamente ocorrido no espaço e no tempo"[27].

Ainda, de acordo com Edilson Mougenot "esse, aliás, [é] o objetivo primordial do chamado processo de conhecimento, no âmbito do qual a parte mais substancial dos atos é voltada à instrução – a produção de provas, a fim de iluminar o espírito do julgador e permitir a ele exercer o poder jurisdicional"[28].

É por meio da persecução penal que o juiz apreciará o material produzido e, aliado aos argumentos trazidos pelas partes, aplicará o direito ao caso concreto – daí porque a importância da prova, possibilitando levar ao julgador o maior número de informações possíveis na reconstrução de determinado fato criminoso.

Diante de tudo isso, é possível ver a importância do estudo da prova e todas as suas implicações e, nesse sentido, a prova digital, hoje, possui papel de extrema relevância, diante das novas tecnologias que maximizaram a obtenção, o armazenamento, a análise e a transmissão de dados.

1.2 PRINCÍPIOS RELACIONADOS À PROVA

Existem limites a serem respeitados na condução do processo penal. Dessa forma, não se pode abster dos princípios – notadamente aqueles relacionados à prova.

Imperioso ressaltar a lição de Eugênio Pacelli acerca da análise dos princípios em si:

> Não custa dar um passo atrás, para *antes* do direito positivado nas ordens jurídicas e, para se entender que a noção de *princípio* utilizada no Direito repousa na ideia de *sistema* e, mais especificamente, na ideia de *sistema jurídico*, isto é, o conjunto de normas de determinado ordenamento, dotado de certa unidade de sentido, sem a qual (a unidade) restaria apenas a pluralidade de normas, no tempo e no espaço, despidas de vínculos interpretativos concretos.
> O direito positivo constitui *sistema* quando se propõe a organizar as leis segundo finalidades mais gerais, reunidas, porém, na identificação e na realização do interesse público e no bem comum. O *Direito* pretende ser a alternativa abstrata da coexistência humana, na medida da maior satisfação possível das necessidades de todos.
> O que efetivamente *amarra* esse conjunto de normas em uma mesma direção é o que se impõe como *sistema* de direitos e deveres recíprocos, destinado a organizar a ordem jurídica, com a explicitação dos valores acolhidos nas normas e com o objetivo de tornar seguras e previsíveis as soluções dos conflitos inerentes à vida comunitária.
> E caberá à *dogmática jurídica* construir os conceitos e as categorias jurídicas necessárias à operacionalização do sistema, de modo a bem cumprir sua essencial função, que, a um só tempo, pretende ser *prescritiva* (proibição de condutas e compatibilização dos direitos) e eficaz, sancionatório, se necessário. No Direito Penal,

[27] PACELLI, Eugênio. **Curso de Processo Penal**. 24. ed. São Paulo: Atlas, 2020. Livro Eletrônico, p. 416.
[28] MOUGENOT, Edilson. **Curso de processo penal**. 13. ed. São Paulo: Saraiva Educação, 2019, p. 468.

> a edificação vem moldada nas normas incriminadoras, para cujo descumprimento é prevista a imposição de sanções.
> Os princípios, portanto, ocupam no sistema jurídico o *andar de cima*, a despeito de suas eventuais deficiências de comando, ou seja, da menor densidade normativa que os caracteriza, o que oferece, em contraponto, maior margem de aplicabilidade, ainda que menos previsível e, por isso mesmo, menos segura.
> Eles se colocam como verdadeiras *premissas* do ordenamento, vinculando a produção legislativa, sobretudo quando se cuidar de princípios de índole constitucional, que são e constituem a grande maioria daqueles utilizados no direito processual penal. Princípio, então, e por assim dizer, configuram a *base*, o *núcleo central* dos sistemas jurídicos[29].

Afinal, como objetivo, a prova consiste na busca da persuasão do julgador, de modo que ele seja capaz de proferir sua decisão com convicção, fundamentado em certeza. Trata-se, portanto, de impactar e moldar a opinião acerca de um fato anterior e que agora está em análise[30] e, dessa forma, imperiosa a observância dos princípios.

1.2.1 Presunção de inocência

Consagrado no art. 5º, inciso LVII, a CF/88, estabelece que "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória", cabendo ao Estado provar a culpa do réu – e não a ele demonstrar sua inocência, estado que lhe é inerente.

Dessa forma, o princípio da presunção de inocência é um dos pilares fundamentais do direito penal e processual penal, e sua relação com o âmbito probatório se vê desde o ônus da prova (que recai sobre a acusação), até o fato de que, para eventual decreto condenatório, devem existir provas suficientes que afastem dúvidas razoáveis sobre a culpa – de modo que, a ausência de provas, levará à absolvição.

E, como consequência, o *in dubio pro reo* não se trata, assim, de mera norma de avaliação das evidências. Na realidade, deve ser aplicado no instante de avaliar as provas: em casos de incerteza, a decisão deve ser favorável ao acusado, já que ele não possui a incumbência de demonstrar que não cometeu o crime[31].

Aliás, a Declaração Universal dos Direitos Humanos estabelece que "todo ser humano acusado de um ato delituoso tem o direito de ser presumido inocente até que a sua culpabilidade tenha sido provada de acordo com a lei, em julgado público no qual lhe tenham sido asseguradas todas as garantias necessárias à sua defesa" (art. 11.1).

---

[29] PACELLI, Eugênio. **Curso de processo penal**. 28. edição. Lumen Juris: Rio de Janeiro, 2024, p. 4-5.
[30] BARRETO, Leonardo; ALVES, Moreira. **Processo Penal Parte Geral**. 10. ed. Salvador: Juspodivm, 2020, p. 359.
[31] LIMA, Renato Brasileiro. **Manual de Processo Penal** – volume único. São Paulo: Juspodivm, 2022, p. 49.

No mesmo sentido, a Convenção Americana sobre Direitos Humanos (Dec. 678/92) que, em seu art. 8º, § 2º estabelece que "toda pessoa acusada de delito em direito a que se presuma sua inocência enquanto não se comprove legalmente sua culpa".

Em outras palavras, o princípio assegura que ninguém será condenado sem a robustez probatória necessária.

1.2.2 Contraditório e ampla defesa

Também são garantias constitucionais fundamentais no processo penal, diretamente ligadas à produção e à avaliação das provas, assegurando o devido processo legal, o contraditório e a ampla defesa, com os meios e recursos a ela inerentes. Dessa forma "ninguém será privado da liberdade ou de seus bens sem o devido processo legal" (art. 5º, inc. LIV, CF/88) e "aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e a ampla defesa, com os meios e recursos a ela inerentes" (art. 5º, LV, CF/88).

Dessa forma, as partes têm oportunidade na produção e manifestação acerca das provas e, em consequência, que sejam assegurados todos os meios disponíveis para defesa. Também guarda relação direta com a inadmissibilidade das provas ilícitas, reforçando a integridade do devido processo legal.

É importante evitar surpresas, não apenas quanto às provas apresentadas, mas também em relação aos aspectos jurídicos que estão sendo discutidos. A questão jurídica nem sempre se resolve por meio de um mero processo de subsunção. Na verdade, é bastante complexo, mesmo que muitas vezes essa complexidade não se manifeste na decisão judicial, que pode parecer simples e automática[32].

Em suma, os fundamentos do contraditório e da ampla defesa são fundamentais para assegurar a igualdade de condições no âmbito do processo penal, garantindo ao acusado a chance de se envolver ativamente na coleta e contestação das evidências apresentadas. Essas não são apenas ferramentas que salvaguardam o direito à defesa, mas também que fortalecem a legitimidade do julgamento, prevenindo decisões fundamentadas em provas unilaterais ou não verificadas (no sentido de questionamentos acerca de sua existência).

[32] BADARÓ, Gustavo Henrique. **Processo Penal**.11. ed., São Paulo: Thomson Reuters Brasil, 2023, p. 63.

Nas lições de Aury Lopes Júnior, o ato de contradizer aquela argumentação trazida à baila como verdade pela acusação, "é ato imprescindível para um mínimo de configuração acusatória do processo"[33].

O cumprimento desses princípios reforça o devido processo legal, pilar do sistema penal democrático.

1.2.3 A busca pela verdade real

A busca pela verdade real implica na responsabilidade do Estado (representado na figura do julgador) de apurar e identificar os fatos de forma que reflitam a realidade da maneira mais acurada possível.

Como já dito outrora, ao contrário do processo civil, que se baseia na noção de verdade formal (ou seja, o que é apresentado como prova pelas partes dentro das normas estabelecidas), o enfoque no processo penal é mais abrangente, visando esclarecer os eventos ocorridos, para que a decisão (absolutória ou condenatória) seja a mais justa e exata possível. Assim, enquanto no âmbito cível o magistrado é um espectador da prova, no âmbito criminal atuará na busca dos elementos probatórios[34].

Dessa forma, o principal propósito da prova no âmbito penal é atuar como um instrumento para elucidação dos eventos, possibilitando que o magistrado forme sua convicção fundamentada na realidade dos fatos, em vez de se apoiar em suposições ou unicamente nas alegações das partes envolvidas.

De acordo com Guilherme de Souza Nucci:

> A análise desse princípio inicia-se pelo conceito de verdade, sempre de caráter relativo, até findar com a conclusão de que há impossibilidade real de se extrair, nos autos, o fiel retrato da realidade do crime. Diante disso, jamais, no processo, pode assegurar o juiz ter alcançado a *verdade objetiva*, aquela que corresponde perfeitamente com o acontecido no plano real. Tem, isto sim, o magistrado uma crença segura na verdade, que transparece através das provas colhidas e, por tal motivo, condena ou absolve.
> [...]
> Não questionamos ser a verdade uma e sempre relativa, consistindo busca inviável, no processo, encontrar a *realidade* dos fatos tal como ocorreram. A verdade é apenas uma noção ideológica da realidade, motivo pelo qual o que é verdadeiro para uns, não o é para outros [...][35].

---

[33] LOPES Júnior, Aury. **Direito Processual Penal**. 21. edição. São Paulo: Saraivajur, 2024, p. 81.
[34] NUCCI, Guilherme de Souza. **Manual de Processo Penal – Volume Único**. 5. ed. Rio de Janeiro: Forense, 2024, p. 18.
[35] NUCCI, loc. cit.

A busca da verdade, embora crucial, enfrenta restrições em função do respeito aos direitos fundamentais, sobretudo em relação ao princípio da presunção de inocência. Em outras palavras, não se pode usar de tortura, por exemplo, a pretexto de encontrar a verdade, ainda que essa fosse "real" (ou, por assim dizer, mais aproximativa da realidade).

O processo legal requer que a verdade seja obtida por meio de métodos válidos, ou seja, de acordo com os basilares constitucionais e disciplinado pela legislação infraconstitucional.

Assim, tal princípio busca garantir que a decisão represente, realmente, a realidade dos fatos de maneira mais aproximativa e, além disso, que a obtenção da prova se dê em harmonia com os direitos fundamentais.

1.2.4 Publicidade das provas

Consagrado no artigo. 5º, inciso LX da Constituição Federal, é assegurado que, salvo exceções legais, todos os atos processuais, incluindo a produção e a avaliação das provas sejam públicos, garantindo assim o controle social e a fiscalização dos atos judiciais, de modo que "a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem".

Ainda, "todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei, se o interesse público o exigir, limitar a presença em determinados atos, às próprias partes e seus advogados, ou somente a estes" (art. 93, IX, da CF/88).

Da mesma forma, "as audiências, sessões e os atos processuais serão, em regra, públicos e se realizarão nas sedes dos juízos e tribunais" (art. 792, primeira parte, CPP).

É, portanto, um dos fundamentos do processo penal democrático, estando ligado à clareza e à disponibilidade das informações do processo, especialmente no que se refere às provas. Noutro giro, está intimamente ligado à transparência no acesso às provas e à garantia do contraditório e ampla defesa.

A publicidade atua, assim, como fundamento essencial não apenas para a validade dos atos processuais, mas também para as decisões proferidas pelo Poder Judiciário[36].

Além disso, como não poderia deixar de ser, aplica-se às provas periciais e técnicas – e, nesse diapasão, também às digitais – tendo em vista que devem ser apresentadas no processo de forma acessível e que permita a análise pelas partes.

[36] LIMA, Renato Brasileiro. **Manual de Processo Penal** – volume único. São Paulo: Juspodivm, 2022, p. 67.

1.2.5. Livre convencimento motivado

O juiz não está vinculado a uma predeterminação legal quanto à valoração da prova, podendo formar seu convencimento de maneira livre, a partir da avaliação dos elementos probatórios colhidos durante o processo (art. 155 do CPP).

Além disso, não obstante a liberdade quanto à apreciação das provas, isso não pode se dar de maneira arbitrária, pois, de todo modo, sempre deverá ser motivado, conforme disciplina o art. 93, IX, da CF/88.

E, como os princípios são apreciados de forma conjunta dentro do sistema, não se pode olvidar do contraditório, que garantirá que as provas apresentadas poderão ser questionadas e debatidas pelas partes.

Diante disso, a livre apreciação das provas garantirá flexibilidade (e, dessa forma, a justiça, no sentido de análise probatória imparcial e aplicabilidade correta das normas legais) no âmbito do processo penal, permitindo que o julgador forme seu convencimento com base nos elementos de prova apresentados, sem que haja hierarquia predeterminada.

Contudo – e aqui já adentrando no debate da prova digital – é necessário cuidado quando da tomada de decisões, especialmente diante de situações em que há evidente lacuna acerca da prova, uma vez que as garantias já consolidadas não podem ser ignoradas.

1.3 ÔNUS DA PROVA

Levando em consideração a ideia de deveres para o campo probatório, é possível afirmar que o ônus da prova é a obrigação que as partes possuem de comprovar, de forma legal e moralmente aceitável, a veracidade das alegações feitas ao longo do procedimento, o que pode resultar em situação de desvantagem caso não o façam.

Nesse sentido, Fernando Capez destaca que:

> [...] a principal diferença entre obrigação e ônus reside na obrigatoriedade. Enquanto na obrigação a parte tem o dever de praticar o ato, sob pena de violar a lei, no ônus o adimplemento é facultativo, de modo que o seu não cumprimento não significa atuação contrária ao direito. Neste último caso, contudo, embora não tenha afrontado o ordenamento legal, a parte arcará com o prejuízo decorrente de sua inação ou deixará de obter a vantagem que adviria de sua atuação[37].

[37] CAPEZ, Fernando. **Curso de Processo Penal**. 5. ed. Saraiva: São Paulo, 2006, p. 377.

Conforme o artigo 156 do CPP, em regra, a prova da alegação incumbirá a quem a fizer[38]. Portanto, extrai-se do texto legal que há efetiva distribuição do ônus da prova entre acusação e defesa[39] e, ainda, que o juiz tem poderes instrutórios no processo penal, mas sempre de forma complementar à atividade das partes.

Edilson Mougenot explica que:

> O processo penal versa sobre fatos, imputados ao réu pelo titular da ação penal. Contra os fatos alegados pelo autor da ação, que deduz a pretensão punitiva em juízo, por meio da denúncia ou da queixa, conforme o caso, é que se defenderá o acusado. Entretanto, somente poderão ser adotados na fundamentação das decisões os fatos que houverem sido efetivamente provados. As regras do ônus da prova visam determinar, em cada situação, a quem incumbe a produção de provas acerca de cada fato.
> Quanto a isso, a regra geral vigente entre nós é a do brocardo latino *actori incumbit probatio*, que em vernáculo se traduz no cânon segundo o qual cabe ao autor a prova do que alegar. O ônus probatório, portanto, representa um encargo que tem a parte de provar as suas alegações, buscando criar no juiz a convicção acerca de sua veracidade. Em regra, cabe ao acusador provar os elementos que compõem a imputação levada a juízo. A esse respeito, é relevante que se diga que a incumbência não constitui um dever: não há sanção, propriamente dita, a ameaçar aquele que não prova o quanto alega. A consequência jurídica da falta de prova acerca daquilo que se alega é o não acatamento da alegação. O autor que não prova o que alega assume, na pior das hipóteses, o risco de ver desatendido sua pretensão. Daí se falar em ônus da prova, em dever de dever de prova ou direito de prova[40].

Ainda, acrescenta Mougenot:

> A regra mencionada, entretanto, não vige solitária. É complementada por outra, consubstanciada no dizer latino *et reus in excipiendo fit actor*, que se traduz na exigência de que o acusado demonstre os fatos que alegue com o fim de elidir a pretensão do autor.
> Sintetizando o que há de comum entre as duas regras, chega-se a uma terceira, segundo a qual a prova dos fatos alegados cabe a quem faz a alegação [...] consubstanciada no art. 156, *caput*, do Código de Processo Penal.
> [...]
> Ainda no tocante ao ônus da prova, deve ser reconhecida a regra da comunhão da prova, já que esta, uma vez produzida, poderá ser valorada pelo julgador independentemente da parte que a produziu [...][41].

Uma vez produzida, a evidência não está sob posse da parte que a apresentou no procedimento, sendo de responsabilidade do juiz avaliar todas as provas disponíveis nos autos,

---

[38] Referido dispositivo destaca ser facultado ao juiz de ofício: I – ordenar, mesmo antes de iniciada a ação penal, a produção antecipada de provas consideradas urgentes e relevantes, observando a necessidade, adequação e proporcionalidade da medida; II – determinar, no curso da instrução, ou antes de proferir a sentença, a realização de diligência para dirimir dúvida sobre ponto relevante.
[39] Nesse sentido, compete ao autor da ação penal demonstrar autoria e materialidade delitiva ao passo que, à defesa, a existência de excludentes e causas de extinção da punibilidade
[40] MOUGENOT, Edilson. **Curso de processo penal**. 14. ed. São Paulo: Saraiva Jur, 2024, p. 289.
[41] Ibid., p. 289-290.

independente de quem as produziu, não podendo, assim, "contentar-se com a verdade formal trazida pelas partes"[42].

De acordo com Gustavo Badaró:

> [...] o ônus da prova funciona como um estímulo para as partes, visando à produção das provas que possam levar ao conhecimento do juiz a verdade sobre os fatos. Em função dessa distribuição dos riscos sobre a não comprovação de um fato, em que se fundamente a pretensão ou a defesa, é que as regras sobre ônus da prova funcionam como uma pressão psicológica para as partes, tendo o efeito de motivá-las a participar ativamente a fornecer a prova dos fatos que pretende ver reconhecidos no processo. As partes são estimuladas a provar suas alegações, ante o risco da prova frustrada[43].

O juiz também possui poderes instrutórios no âmbito do processo penal, o que se evidencia na possibilidade de requerer provas consideradas urgentes, ainda que antes do início da ação penal e, durante a instrução, a realização de diligências para esclarecimento de dúvidas. Referida atuação, reitera-se, é sempre realizada de forma complementar, pois a imparcialidade não pode ser maculada. Em suma, deve o juiz deliberar pela produção de evidências que entender que, naquele caso concreto, sejam pertinentes[44].

Toda essa divisão de tarefas é importante pois, se ao término do procedimento as provas não forem suficientes para que o juiz possa chegar a uma conclusão sobre a validade das alegações de ambas as partes, deverá absolver o réu, conforme o *in dubio pro reo.*

Assim, o debate acerca do ônus da prova – e também da atuação de ofício do juiz – se revela extremamente importante, consideradas as características das evidências digitais, sendo seu estudo ainda recente e, mais do que isso, em constante evolução, o que, na prática, demanda cuidado acerca das garantias individuais há muito conquistadas e que não podem, a pretexto da busca pela solução dentro de um processo, ser desconsideradas, sob pena de, ao final, ter-se o procedimento anulado.

1.4 FONTE DE PROVA, MEIOS DE PROVA E MEIOS DE OBTENÇÃO DE PROVA

O termo fonte de prova é empregado para se referir às pessoas ou objetos que fornecem evidências. Após a ocorrência do crime, qualquer elemento que possa ajudar no esclarecimento acerca de sua existência pode ser considerado uma prova. Essas evidências surgem do ato

---

[42] MOUGENOT, Edilson. **Curso de processo penal**. 14. ed. São Paulo: Saraiva Jur, 2024, p. 290.
[43] BADARÓ, Gustavo Henrique. **Ônus da prova no processo penal**. São Paulo: Editora Revista dos Tribunais, 2003, p. 182.
[44] NUCCI, Guilherme de Souza. **Manual de Processo Penal**. Volume Único. 5. ed. Rio de Janeiro: Forense, 2024, p. 239.

delitivo em si, mesmo antes do início do processo, sendo introduzidas no caso através dos meios de prova.

Em suma, o que for apto a permitir a produção de determinada prova, será fonte de prova; o instrumento pelo qual aquela evidência é inserida no processo será o meio de prova; e o elemento de prova, aquilo que confirma (ou não) determinada alegação. Por fim, haverá o resultado probatório, que será a conclusão do julgador acerca de tais fontes e elementos obtidos.

Acerca de tais diferenciações, Gustavo Badaró esclarece o seguinte:

> [...] enquanto os **meios de prova** são aptos a servir, **diretamente**, ao convencimento do juiz sobre a veracidade ou não de uma afirmação fática (por exemplo, o depoimento de uma testemunha, ou o teor de uma escritura pública), os meios de obtenção de provas (por exemplo, uma busca e apreensão) são instrumentos para a colheita de elementos ou fontes de provas, estes, sim, aptos a convencer o julgador (por exemplo, um extrato bancário [documento] encontrado em uma busca e apreensão domiciliar). Ou seja, enquanto o meio de prova se presta ao convencimento direto do julgador, **os meios de obtenção de provas** somente **indiretamente**, e dependendo do resultado de sua realização, poderão servir à reconstrução da história dos fatos.
> Em regra, os meios de obtenção de prova implicam restrição a direitos fundamentais do investigado, em geral liberdades públicas ligadas à sua privacidade ou intimidade ou à liberdade de manifestação do pensamento. É o que ocorre na quebra de sigilo bancário ou fiscal, em que há restrição à intimidade (CR, art. 5º, *caput*, X), na busca domiciliar, que implica restrição à inviolabilidade do domicílio (CR, art. 5º, *caput*, XI), ou, ainda, à interceptação telefônica, realizada como exceção constitucionalmente prevista à liberdade de comunicação telefônica (CR, art. 5º, *caput*, XII)[45].

Dessa forma, cometido um crime em determinado local, as pessoas que presenciaram o fato, por exemplo, serão consideradas fonte de prova; se forem levadas à juízo como testemunhas, suas declarações serão os meios de prova. Estes podem, por sua vez, ser lícitos ou ilícitos e, nesse sentido, o artigo 157 do CPP estabelece que "são inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais". Tal fato guarda estrita observância aos preceitos constitucionais, notadamente o art. 5º, inciso LVI, da CF/88 que determina expressamente que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos".

Nesse diapasão, a prova é adquirida e incluída no processo. Contudo, é necessário seguir de forma estrita método e protocolo, em respeito ao devido processo legal e aqui tem-se os chamados meios de obtenção de prova, que são aqueles procedimentos para obter as evidências no processo penal.

É fundamental diferenciar meios de obtenção de prova e meios de prova, principalmente no que diz respeito às repercussões no procedimento. Isso ocorre porque, se houver alguma

[45] BADARÓ, Gustavo. **Processo Penal**.11. ed. São Paulo: Thomson Reuters Brasil, 2023, p. 381.

falha nos meios de prova, isso acarretará a invalidação da evidência apresentada; porém, se houver alguma irregularidade no meio de obtenção da prova, o resultado será a declaração de sua inadmissibilidade e consequente exclusão do processo[46].

Nesse sentido, Nucci destaca o princípio do devido processo legal, que trata da obediência às normas processuais e suas garantias, de modo que somente estarão devidamente observados "caso todos os princípios norteadores do Direito Penal e do Processo Penal sejam, fielmente, respeitados durante a persecução penal, garantidos e afirmados os direitos do acusado para produzir sua defesa, bem como fazendo atuar um Judiciário imparcial e independente"[47].

Dessa forma, pode-se distinguir inclusive as provas dos elementos informativos, sendo aquelas produzidas sob o crivo do contraditório no bojo de um processo e estes colhidos durante toda a investigação, por qualquer meio (seja no inquérito policial, pelo Ministério Público (MP) em procedimento investigatório ou qualquer outra investigação preliminar).

E, no que diz respeito à evidência eletrônica, é necessário que o devido processo legal autorize a obtenção das provas conforme a legislação, sempre com respeito à soberania do país. Portanto, se a prova digital for obtida dentro dos padrões legais, ela deve ser aceita como válida para todos os efeitos formais e substanciais.

1.5 PROVAS ATÍPICAS

A análise sobre fontes, meios e elementos de prova e, consequentemente, a questão da evidência digital, culmina em outro ponto de interessante debate: poder-se-ia admitir a aplicação de provas atípicas no âmbito do processo penal que, em última análise, irá desaguar na possibilidade de restrição de liberdade do indivíduo?

Nesse sentido, o artigo 369 do Código de Processo Civil (CPC) disciplina que "As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz".

A aplicação do CPC de forma subsidiária é permitida, sendo que o artigo 3º do Código de Processo Penal estabelece que "A lei processual admitirá interpretação extensiva e aplicação analógica, bem como o suplemento dos princípios gerais de direito".

---

[46] COSTA, Klaus Negri; ARAÚJO, Fábio Roque. **Processo Penal Didático**. 3. ed. Salvador: Juspodivm, 2020, p. 519.

[47] NUCCI, Guilherme de Souza. **Princípios constitucionais penais e processuais penais**. 4. ed. Rio de Janeiro: Forense, 2015, p. 148.

Nesse sentido, o entendimento do Colendo Superior Tribunal de Justiça:

> [...] as normas de processo civil aplicam-se de forma subsidiária ao processo penal. Nesse sentido, observe-se o teor do art. 3º do Código de Processo Penal. A jurisprudência desta Corte, seguindo a doutrina majoritária, admite a aplicabilidade das normas processuais civis ao processo penal, desde que haja lacuna a ser suprida. Importante ressaltar que a lei processual penal não tratou, detalhadamente, de todos os poderes conferidos ao julgador no exercício da jurisdição [...][48].

As provas atípicas são aquelas obtidas de forma não convencional, como as testemunhais ou periciais. Afinal, o CPP não apresenta rol taxativo dos meios de prova lícitos, razão pela qual aquelas disciplinadas nos artigos 158 a 250 do CPP são os meios típicos (nominados). Assim, a inclusão de provas atípicas no decorrer do processo poderia ser aceita, considerando-se as garantias do contraditório e da ampla defesa, com a eficiência máxima dos meios de prova disponíveis.

Sobre o tema, Gustavo Badaró faz a seguinte ponderação:

> É controvertido, contudo, o que se deve entender por **prova atípica**. Inicialmente, não se pode confundir tipicidade probatória, entendida como a **previsão de um procedimento probatório típico** para a produção de um determinado meio de prova, com a simples **nominação de uma prova**. Por exemplo, o CPP faz referência à "reprodução simulada dos fatos" (art. 7º), vulgarmente conhecida como "reconstituição do crime". Não lhe indica, porém, nenhum procedimento.
> Nos casos em que a lei estabelece um determinado procedimento para a produção de uma prova, o respeito dessa disciplina legal assegura a genuinidade e a capacidade demonstrativa de tal meio de prova. Toda vez que tal procedimento probatório não é seguido, o problema que se coloca não é saber se o meio de prova produzido é típico ou atípico, mas sim se os requisitos e condições previstos em lei, mas que não foram observados na admissão ou produção da prova, eram ou não essenciais para tal meio probatório[49].

Por tal razão, a utilização de provas atípicas deve ser feita com acuidade, em análise do caso concreto e respeitando as garantias constitucionais, como a proporcionalidade, afinal, não se pode, sob o argumento de busca de uma verdade, ignorar que a restrição aos direitos fundamentais deve ser proporcional àquilo que se pretende provar.

Portanto, quaisquer meios de provas - sejam típicos ou atípicos - devem, sobremaneira, estar em estrita consonância com o ordenamento jurídico, pois para a prova ser efetivamente considerada elemento de prova e inferir no resultado probatório válido, deve ser lícita e obedecer aos critérios de admissibilidade.

---

[48] BRASIL. Superior Tribunal de Justiça. **REsp 1.568.445/PR**, relator Ministro Rogério Schietti Cruz, relator para acórdão Ministro Ribeiro Dantas, Terceira Seção, julgado em 24/6/2020, DJe de 20/8/2020.
[49] BADARÓ, Gustavo. **Processo Penal**.11. ed. São Paulo: Thomson Reuters Brasil, 2023, p. 384-385.

Assim, mesmo a prova atípica não pode se desvincular de preceitos já estabelecidos, garantindo, dessa forma, um processo justo e equitativo. Nesse sentido, Badaró destaca que é necessário distinguir a prova atípica da "irritual", ou seja, aquela "produzida sem a observância de seu procedimento probatório. Por exemplo, em um reconhecimento pessoal, suprimir a primeira fase, de descrição da pessoa a ser reconhecida, havendo um mero apontamento do acusado"[50].

Em vista disso, a questão é de grande relevância, uma vez que a discussão sobre os diferentes tipos de provas não convencionais e sua admissibilidade, diante da tecnologia e da prática de delitos pelos mais variados meios, passa a ter amplo debate no que diz respeito à sua admissibilidade, especialmente quando há colisão com os direitos fundamentais, afinal, no mais, o que se quer é a obtenção da prova de maneira a sustentar – e não prejudicar – a validade do processo.

1.6 PROVAS ILÍCITAS

O artigo 5º, inciso LVI da CF/88 estabelece que não são admissíveis, no processo, as provas obtidas por meios ilícitos.

Ainda, de acordo com o artigo 157, caput, do CPP "são inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais".

Nesse sentido, o modo como a prova é produzida será determinante para a caracterização da sua licitude.

Imperioso destacar que o Código de Processo Penal não faz distinção acerva da *prova ilegítima* e da *prova ilícita,* vez que não estabelece se a norma violada é material ou processual.

Gustavo Badaró, no entanto, destaca diversos pontos acerca da sua distinção. Nesse sentido, em relação ao *momento*, será ilícita quando o vício ocorrer no momento da obtenção, ao passo que, na prova ilegítima, a ilegalidade ocorrerá na produção como, por exemplo, quando se indefere pergunta à testemunha[51]. Ainda, ressalta que:

> [...] Embora normalmente a ilicitude se dê relativamente à obtenção de uma prova, isto é, durante a execução de um meio de obtenção de prova (por exemplo, uma interceptação telefônica ou busca e apreensão), é possível que a ilicitude ocorra no próprio processo, durante a produção da prova. Basta pensar em um acusado que seja torturado, ou submetido à hipnose, ou compelido a tomar o "soro da verdade", durante

[50] BADARÓ, Gustavo. **Processo Penal**.11. ed. São Paulo: Thomson Reuters Brasil, 2023, p. 385.
[51] BADARÓ, Gustavo. **Processo Penal**.11. ed., São Paulo: Thomson Reuters Brasil, 2023, p. 398-399.

> seu interrogatório. Haverá ilicitude na produção de um meio de prova durante a instrução processual. Se um padre prestar depoimento sobre algo que teve conhecimento durante uma confissão, o vício que acarretará a ilicitude da prova testemunhal se dará na própria produção do meio da prova[52].

Badaró também estabelece as seguintes conceituações acerca de tais distinções dos pontos de vista *material* e quanto à sanção *processual*:

> [...] do ponto de vista do material que poderá ser valorado para a formação do convencimento judicial, não terá maiores reflexos a distinção entre prova ilícita e prova ilegítima, na medida em que, tanto a prova **obtida ilicitamente** quanto a **prova produzida ilegitimamente não poderá ser valorada pelo juiz**. Não se pode ignorar que as regras sobre admissão e produção da prova têm por escopo último uma correta seleção do material que poderá ser valorado pelo juiz para a formação de seu convencimento.
> Por outro lado, quanto à sanção processual, afirma-se que a prova ilícita é **inadmissível**, o que evita o seu ingresso no processo, enquanto a prova ilegítima será sancionada com a **nulidade** de sua produção, uma sanção, portanto, *ex post factum*. Além disso, a prova ilícita não pode ser renovada, enquanto em relação à ilegítima "impõe a necessidade de sua renovação, nos termos do que determina o art. 573 do CPP"[53].

O que se pode concluir é que existem as provas ilegais, que são o gênero do qual as provas ilegítimas e as ilícitas fazem parte. As ilegítimas são aquelas obtidas em dissonância ao direito processual, ao passo que as ilícitas são aquelas obtidas em violação a normas constitucionais ou legais[54] e, não apenas estas devem ser inadmissíveis - e consequentemente desentranhadas do processo -, mas também aquelas derivadas das ilícitas, nos termos do art. 157, § 1º, do CPP, sendo as chamadas "provas ilícitas por derivação", consagrando, no direito brasileiro, a Teoria dos Frutos da Árvore Envenenada (*Fruits of Poisonous Tree*). No entanto, essa irregularidade só será confirmada se houver comprovação da conexão entre as evidências ou quando as informações secundárias não puderem ser obtidas por uma fonte neutra em relação às primeiras.

Nesse sentido, Renato Brasileiro esclarece:

> De nada adianta dizer que são inadmissíveis, no processo, as provas obtidas por meios ilícitos se essa ilicitude também não se estender às provas que dela derivam. Com efeito, a admissibilidade no processo de provas ilicitamente derivadas poderia servir de expediente para contornar a vedação probatória do art. 5º, LVI, da Constituição Federal, isto é, as partes poderiam sentir-se encorajadas a recorrer a expedientes ilícitos com o objetivo de se servir de elementos de prova até então inatingíveis pelas vias legais [...] Provas ilícitas por derivação são os meios probatórios que, não obstante produzidos, validamente, em momento posterior, encontram-se afetados pelo

[52] BADARÓ, Gustavo. **Processo Penal**.11. ed., São Paulo: Thomson Reuters Brasil, 2023, p. 399.
[53] Ibid., p. 399.
[54] BARRETO, Leonardo; ALVES, Moreira. **Processo Penal Parte Geral**. 10. ed. Salvador: Juspodivm, 2020, p. 367.

> vício da ilicitude originária, que a eles se transmite, contaminando-os, por efeito de repercussão causal. A título de exemplo, suponha-se que alguém tenha sido constrangido, mediante tortura, a confessar a prática de um crime de homicídio. Pode ser que, dessa prova ilícita originária, resulte a localização e apreensão de um cadáver. Apesar de a apreensão do cadáver ser aparentemente lícita, não há como negar que há um nexo causal inequívoco entre a confissão mediante tortura e a localização do cadáver. Em outras palavras, não fosse a prova ilícita originária, jamais teria sido possível a prova que dela derivou. Nessa linha de pensamento, é possível concluir que a ilicitude da prova originária transmite-se, por repercussão, a todos os dados probatórios que nela se apoiem, ou dela derivem, ou, finalmente, nela encontrem o seu fundamento causal[55].

Sob essa ótica, a prova será considerada ilícita caso seja obtida com violação de diretrizes legais ou princípios fundamentais do sistema, tanto de forma material quanto processual – aqui, com destaque a diversos direitos elencados na CF/88 como inviolabilidade do domicílio (art. 5º, XI), inviolabilidade do sigilo das comunicações e dos dados (art. 5º, XII), inviolabilidade da intimidade, da vida privada, da imagem e da honra (art. 5º, X), respeito à integridade física e moral do preso (art. 5º, XLIX), vedação ao emprego de tortura ou tratamento desumano ou degradante (art. 5º, III), dentre outros[56].

Por outro lado, será ilegítima quando obtida com violação à norma de direito processual penal. Como exemplo, pode-se imaginar reconhecimento realizado sem a observância do art. 226 do Código de Processo Penal ou exibição de documentos no plenário do júri sem que tenham sido juntados com a antecedência mínima de três dias úteis, conforme art. 479 do Código de Processo Penal e, se assim for feito, será reconhecida sua ilegitimidade[57].

Portanto, em relação ao tratamento das provas ilícitas e ilegítimas, dentro da legislação nacional, por mais importantes que sejam os acontecimentos descobertos por provas obtidas de forma ilegal, estas não podem ser aceitas no processo. Caso uma prova ilícita seja inserida, surge o direito de exclusão, que pode ser realizado através da remoção dos autos.

O Supremo Tribunal Federal (STF), em mais de uma ocasião, já reconheceu a teoria dos frutos da árvore envenenada, como se vê no julgamento do RHC 235290, relatado pelo Min. André Mendonça e publicado em 14/06/2024:

> Agravo Regimental no Recurso Ordinário em Habeas Corpus. Tráfico de Drogas. art. 5º, inc. XI, da CRFB. Inviolabilidade domiciliar: desrespeito. Fundadas razões para ingresso dos policiais: inexistência. Ilegalidade manifesta. 1. A entrada desautorizada e desacompanhada de mandado judicial em residência particular só se justifica quando existentes fundadas razões da ocorrência de situação de flagrante delito, observado o que dispõe o art. 5º, inc. XI, da CFRB, nos termos do Tema nº 280 do ementário da

[55] LIMA, Renato Brasileiro. **Manual de Processo Penal** – volume único. São Paulo: Juspodivm, 2022, p. 600-601.
[56] LIMA, loc. cit.
[57] LIMA, loc. cit.

> Repercussão Geral. 2. A existência de indícios, sem conexão segura, de prática delitiva, em local incerto e por pessoa desconhecida, não autoriza o ingresso desautorizado em domicílio. 3. A constatação do flagrante, sem justificação prévia da sua ocorrência, é desinfluente, não infirmando a conclusão no sentido da ocorrência da nulidade. 4. A ilegalidade da diligência revela a ilicitude dos elementos dela oriundos e implica, observados o art. 157 do Código de Processo Penal e a teoria dos frutos da árvore envenenada (fruits of poisonous tree), a contaminação dos atos que se seguiram. 5. O vício, por envolver a comprovação da materialidade do crime, resulta na insubsistência da condenação. 6. Agravo regimental do Ministério Público Federal ao qual se nega provimento.

O C. Superior Tribunal de Justiça também assim o reconhece. Nesse sentido, a Quinta Turma, no julgamento do HC 828.054, de relatoria do Min. Joel Ilan Paciornik, julgado em 23/04/2024, por unanimidade, decidiu que são inadmissíveis no processo penal as provas obtidas de celular se não tiverem sido adotados os procedimentos necessários para assegurar a idoneidade e a integridade dos dados extraídos, notadamente porque as provas digitais podem ser facilmente alteradas.

Considerando-se que a prova ilícita não pode gerar outra (ou outras) que se tornem lícitas, ao contrário, todas as que advierem da ilícita são igualmente inadmissíveis, a única exceção concentra-se na prova de fonte independente que, segundo Guilherme de Souza Nucci é aquela que não se abala pela ilegalidade presente em evidência relacionada[58]. O autor traz o seguinte exemplo elucidativo:

> Imagine-se que, por escuta clandestina, logo ilegal, obtém-se a localização de um documento incriminador em relação ao indicado. Ocorre que, uma testemunha, depondo regularmente, também indicou à polícia o lugar onde se encontrava o referido documento. Na verdade, se esse documento fosse apreendido unicamente pela informação surgida da escuta, seria prova ilícita por derivação e inadmissível no processo. Porém, tendo em vista que ele teve fonte independente, vale dizer, seria encontrado do mesmo modo, mesmo que a escuta não tivesse sido feita, pode ser acolhido como prova ilícita[59].

Conforme estabelece o artigo 157, § 2º, do CPP, "considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova".

Eugênio Pacelli, acerca das provas ilícitas, assim discorre:

> Mais que uma afirmação de propósitos éticos no trato das questões do Direito, as aludidas normas, constitucional e legal, cumprem uma função ainda mais relevante, particularmente no que diz respeito ao processo penal, a saber: a vedação das provas ilícitas atua no controle da regularidade da atividade estatal persecutória, inibindo e

[58] NUCCI, Guilherme de Souza. **Manual de Processo Penal**. Volume Único. 5. ed. Rio de Janeiro: Forense, 2024, p. 237.
[59] NUCCI, loc. cit.

> desestimulando a adoção de práticas probatórias ilegais por parte de quem é o grande responsável pela sua produção. Nesse sentido, cumpre função eminentemente *pedagógica*, ao mesmo tempo que tutela determinados valores reconhecidos pela ordem jurídica.
> A norma assecuratória da inadmissibilidade das provas obtidas com violação de direito, com efeito, presta-se, a um só tempo, a tutelar direitos e garantias individuais, bem como a própria qualidade do material probatório a ser introduzido e valorado no processo.
> [...]
> No que se refere à questão da *qualidade* da prova, o reconhecimento da ilicitude *do meio* da obtenção da prova já impede o aproveitamento de métodos cuja idoneidade probatória seja previamente questionada, como ocorre, por exemplo, na confissão obtida mediante tortura, ou mediante hipnose, ou, ainda, pela ministração de substâncias químicas (soro da verdade etc.) De outro lado, a vedação das provas obtidas ilicitamente também oferece repercussão no âmbito da igualdade processual, no ponto em que, ao impedir a produção probatória irregular pelos agentes do Estado – normalmente os responsáveis pela prova -, equilibra a relação de forças relativamente à atividade instrutória desenvolvida pela defesa.
> Na realidade, o tema da inadmissibilidade das provas ilícitas oferece inúmeros desdobramentos, não só no âmbito da prova, como também no campo da própria concepção do Direito que haverá de relevar o intérprete, por ocasião da tarefa hermenêutica [...][60].

A possibilidade de admissão da prova ilícita desde que em benefício ao réu (*pro reo),* ainda é um tema que gera debate. Nesse sentido, explica Fernando Capez que:

> Para justificar a utilização da prova ilícita produzida em ofensa direta ao texto constitucional, o princípio da proporcionalidade admite a manutenção da prova ilícita no processo penal, quando o direito violado for inferior ao valor que se quer proteger com a admissão da prova ilícita. Doutrinariamente, há divisão entre aqueles que admitem o princípio da proporcionalidade para todos os casos e os que o justificam apenas *pro reo.* Nesse contexto, o direito à liberdade e a necessidade de corrigir punições injustas ganharia dimensão superior ao da higidez processual, podendo o réu valer-se de meios heterodoxos para comprovar sua inocência e manter sua garantia constitucional de liberdade. Pode-se dizer: *male captum, bene retentum* (mal recolhida, mas bem recebida), razão pela qual sua admissibilidade seria uma forma de romper, em prol do direito de defesa, com a imutabilidade da vedação constitucional da prova ilícita[61].

No entanto, Capez conclui que:

> A regra deve ser mesmo a da inadmissibilidade das provas obtidas ilicitamente, mesmo que seja em benefício do réu, tendo em vista a relevância da garantia constitucional que a proíbe: "são inadmissíveis, no processo, as provas obtidas por meio ilícito" (CF, art. 5º, LVI). A legislação processual, inclusive, determina seu desentranhamento do processo (CPP, art. 157). Assim, o réu não pode valer-se de provas ilícitas em sua defesa. Há que se ressaltar, porém, que em direito, enquanto ciência normativa e valorativa, nada deve ter caráter absoluto e intransponível. Se a prova ilícita for o único meio de evitar que um inocente seja condenado, não há regra

[60] PACELLI, Eugênio. **Curso de processo penal**. 28. edição. Lumen Juris: Rio de Janeiro, 2024, p. 294-295.
[61] CAPEZ, Fernando. Uso de prova ilícita para evitar que um inocente seja condenado. **ConJur,** 24 ago. 2023. Disponível em: https://www.conjur.com.br/2023-ago-24/controversias-juridicas-provas-ilicitas-inocencia/. Acesso em: 1 fev. 2024.

> jurídica capaz de fechar os olhos à verdade que se apresenta, ainda que sob o pecado original da ilicitude. No processo penal, mecanismo de imposição do mais estigmatizante, invasivo e traumático ramo do ordenamento legal, nada suplanta o valor de comprovar a inocência de alguém injustamente acusado[62].

Em contrapartida, Aury Lopes Júnior trata a possibilidade de ser admitida a prova ilícita a partir da proporcionalidade *pro reo*, pois a ponderação entre o direito de liberdade de um inocente "prevalece sobre um eventual direito sacrificado na obtenção da prova (dessa inocência)"[63]. Além disso, ressalta que:

> Desnecessário argumentar que a condenação de um inocente fere de morte o valor "justiça", pois o princípio supremo é o da proteção dos inocentes no processo penal.
> Ademais, deve-se recordar que o réu estaria, quando da obtenção (ilícita) da prova, acobertado pelas excludentes da legítima defesa ou do estado de necessidade, conforme o caso. Também é perfeitamente sustentável a tese da inexigibilidade de conduta diversa (excluindo agora a culpabilidade). Tais excludentes afastariam a ilicitude da conduta e da própria prova, legitimando seu uso no processo[64].

No entanto, Aury Lopes Júnior também destaca que essa prova não poderia ser usada para, em outro processo penal, punir terceiros:

> [...] na medida em que, em relação a ele, essa prova é ilícita e assim deve ser tratada (inadmissível, portanto). Não há nenhuma contradição nesse tratamento, na medida em que a prova ilícita está sendo, excepcionalmente, admitida para evitar a injusta condenação de alguém (proporcionalidade).
> Essa admissão está vinculada a esse processo.
> Não existe uma convalidação, ou seja, ela não se torna lícita para todos os efeitos, senão que apenas é admitida em um determinado processo (em que o réu a obteve atua ao abrigo do estado de necessidade). Ela segue sendo ilícita e, portanto, não pode ser utilizada em outro processo para condenar alguém, sob pena de, por via indireta, admitirmos a prova ilícita contra o réu (sim, porque ele era "terceiro" no processo originário, mas assume agora a posição de réu).
> Tampouco pode ser invocada a proporcionalidade (contra o réu) [...] Em definitivo, não pode ser utilizada contra terceiro, pois frente a ele essa prova continua ilícita [...][65].

No mais, o artigo 157, § 3º do CPP determina que da decisão do juiz, ao proferir decisão determinando o desentranhamento de prova ilícita, cabível impugnação; preclusa a questão, é facultado às partes acompanhar o incidente para sua destruição.

Por fim, a Lei nº 13.964/19 (Pacote Anticrime) incluiu o § 5º ao artigo 157 do CPP, determinando que "o juiz que conhecer do conteúdo da prova declarada inadmissível não

---

[62] CAPEZ, Fernando. Uso de prova ilícita para evitar que um inocente seja condenado. **ConJur,** 24 ago. 2023. Disponível em: https://www.conjur.com.br/2023-ago-24/controversias-juridicas-provas-ilicitas-inocencia/. Acesso em: 1 fev. 2024.
[63] LOPES Júnior, Aury. **Direito Processual Penal**. 21. edição. São Paulo: Saraivajur, 2024, p. 463.
[64] Ibid., p. 464.
[65] Ibid., p. 464-465.

poderá proferir a sentença ou acórdão". No entanto, o STF considerou o dispositivo inconstitucional, por entender que a norma viola os princípios do juiz natural, da legalidade e da razoabilidade, porquanto ausentes elementos claros e objetivos para a seleção do juiz sentenciante. Dessa forma, reconhecida, portanto, a inconstitucionalidade material da norma em questão[66].

Fato é que toda essa análise das características da prova - e sua consequente utilização - deve ser conduzida à prova digital que deverá também ser produzida em consonância com as normas constitucionais, tratados e convenções internacionais de que o Brasil faça parte, além daquelas infraconstitucionais.

Em um segundo momento – como se verá adiante – é de rigor analisar as peculiaridades que a prova digital traz em seu âmago, daí porque exige maior cautela durante sua produção e consequente manuseio, o que conduz a mais uma observação: o estudo da viabilidade de normas específicas acerca da prova digital.

Antes de adentrar no campo da prova digital propriamente dita, é importante tecer considerações sobre como a internet e as novas formas de interação humana podem se desdobrar quando considerados os direitos e garantias fundamentais, afinal, toda a coleta de informações deve, sobretudo, observar – e respeitar – tais pontos.

[66] BRASIL. Supremo Tribunal Federal. ADI 6.298/DF, ADI 6.299/DF, ADI 6.300/DF e ADI 6.305/DF, Rel. Min. Luiz Fux, julgados em 24/08/2023.

2 O PROCESSO NA ERA DIGITAL: IMPACTOS E DESAFIOS CONSTITUCIONAIS

2.1 A INTERNET COMO AGENTE DE TRANSFORMAÇÃO: PROTEÇÃO E COLISÃO DE DIREITOS FUNDAMENTAIS

O direito encontra-se em constante evolução, sendo um reflexo das necessidades da sociedade. Contudo, as mudanças de paradigmas ocorrem em uma velocidade avassaladora, o que demanda, por vezes, tortuosa hermenêutica diante da análise de diversos direitos e garantias constitucionais colocadas em xeque.

Nesse sentido, a era da informação trouxe transformações significativas nas relações entre instituições e pessoas. A chegada da *internet* e das novas tecnologias está tão imersa nas experiências individuais e coletivas que, hoje, é difícil avaliar determinados aspectos da vida social de modo totalmente dissociado das estruturas tecnológicas.

Diante disso, é possível afirmar que a sociedade vivencia uma nova era, a digital. E, dentro desse contexto, os direitos fundamentais passam por mudanças e desafios. Afinal, não apenas as relações pessoais, como também as empresariais ocorrem dentro do meio digital, com coleta e utilização de dados sensíveis.

A *internet* possibilitou uma expansão considerável; a liberdade de expressão, por exemplo, adquiriu um novo significado, permitindo que pessoas expressem suas ideias e participem ativamente de discussões sobre diversos assuntos de relevância social.

Entretanto, a era digital traz consigo também limitações e obstáculos quando considerados esses direitos fundamentais.

A salvaguarda da privacidade e da segurança das informações pessoais se transformou em uma preocupação permanente, pois a coleta e o uso inadequado desses dados por empresas e instituições governamentais podem comprometer, por exemplo, a intimidade e a vida privada, com obtenção e envio indiscriminado de informações, sem que as implicações legais associadas e os danos ocasionados a indivíduos e/ou empresas sejam considerados[67].

Ademais, a regulamentação da *internet* e a atribuição de responsabilidades são assuntos intrincados que exigem análises e discussões em torno da atuação governamental, da liberdade das empresas de tecnologia e dos direitos dos usuários dentro de toda a estrutura econômico-digital.

[67] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 61.

Aqui ocorre um novo e importante recorte metodológico, pois a temática em questão envolve a análise da proteção dos direitos já consolidados como fundamentais, a exemplo da privacidade, intimidade, honra e imagem, razão pela qual não haverá um estudo detalhado quanto às suas origens.

De todo modo, trata-se do conjunto de direitos considerados fundamentais para os integrantes de uma sociedade em um determinado momento histórico, reconhecidos e respaldados pela Constituição, que possibilitam sua reivindicação e prática, individual ou coletivamente[68]. E, nessa linha, não é possível restringir os direitos fundamentais a um rol taxativo, pois quando a realidade apresenta novas dimensões, estabelecer limites pode levar a equívocos para aqueles que tentarem fazê-lo[69].

Fato é que desde a Declaração Universal dos Direitos Humanos (1948), tem-se a garantia de que "ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação", e que "todo ser humano tem direito à proteção da lei contra tais interferências ou ataques" (art. 12). Além disso, a Constituição Federal (CF/88), no artigo 5º, inciso X, estabelece que são "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

Bomfatti e Kolbe ressaltam que:

> A intimidade pode ser entendida como a esfera mais íntima ou particular de um ser humano; corresponde ao interior do próprio indivíduo, que muitas vezes ele não compartilha com ninguém. É algo dele, que morre com ele, sem que ninguém – ou quase ninguém – saiba, nem mesmo as pessoas de seu núcleo familiar mais próximo, como esposa ou marido. Por sua vez, a ideia de vida privada traduz não o interior do indivíduo, mas o relacionamento entre seus familiares. É algo acima da intimidade, o qual só partilhado entre um número reduzido de pessoas, usualmente do núcleo familiar (esposa, filhos e alguns amigos íntimos) [...] Essa disposição reflete uma questão sempre importante ao *Homo sapiens* de qualquer país do mundo, que é de preservar sua intimidade e a sua vida privada – afinal, ninguém gosta de ser bisbilhotado[70].

Diante disso, vê-se que a intervenção em tais direitos, a despeito de ser possível, deve ser detidamente analisada, para que não tenha seu alcance reduzido, em verdadeiro retrocesso

---

[68] MOTTA, Sylvio. **Direito Constitucional.** 29. ed. Rio de Janeiro: Método, 2021, *E-Book*, p. 211, ISBN 9788530993993. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530993993/. Acesso em: 18 out. 2024.

[69] SALEME, Edson R. **Direito constitucional**. 5. ed. Barueri: Manole, 2022. *E-book*. p.137. ISBN 9786555766370. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555766370/. Acesso em: 07 jun. 2024.

[70] BOMFATI, Cláudio Adriano; KOLBE, Armando Júnior. **Crimes cibernéticos**. Curibita: Intersaberes, 2020, p. 68-69.

que não pode acontecer. Nesse sentido, o princípio da razoabilidade ou da proporcionalidade entra em ação para definir os limites da norma restritiva, ressaltando a importância de manter intacto o núcleo fundamental do direito individual que foi estipulado[71].

Manuel Monteiro Guedes Valente aponta a existência de uma "metamorfose jurídica necessária", destacando a necessidade de um olhar que entenda o ser humano, hoje, verdadeiramente, como ser digital[72]. No entanto, ao analisar tal ponto sob o prisma do direito, isso reflete como ainda é necessário pensar em toda a (ausência) de estrutura. O autor destaca que a metamorfose indica um caminho a se percorrer, diante de uma nova dinâmica presente, destacando que:

> Hoje as pessoas pensam que podem escrever e dizer tudo nas redes sociais por considerarem que estão em um Estado de [total] liberdade de expressão, olvidando, assim, que os limites se extinguem com a afirmação de cada um dos nossos [seus] direitos fundamentais pessoais. O direito de liberdade de expressão e o direito e à informação não são ilimitados. Aceção que muitas vezes os seres digitais esquecem e embarcam na onda que todos pensam conseguir surfar[73].

Afinal, não se pode perder de vista a irradiação do direito constitucional[74] para todo o ordenamento jurídico, razão pela qual a vertente da prova deve ser analisada, precipuamente, diante dos parâmetros há muito tempo conquistados, sob pena de evidente retrocesso, o que não pode ser admitido.

Como ressalta Virgílio Afonso da Silva, os direitos fundamentais constituem verdadeiro sistema de valores:

> Um grande avanço na teoria geral dos direitos fundamentais no pós-guerra foi, sem dúvida alguma, a consolidação definitiva da ideia segundo a qual as declarações de direitos fundamentais não são meras "declarações de princípios", mas contêm verdadeiras normas jurídicas que, pelo menos no que tange às liberdades públicas, conferem direitos subjetivos aos indivíduos.
> Mas uma outra mudança de paradigma no âmbito dos direitos fundamentais, também ocorrida na segunda metade do século XX, teve importância ainda mais decisiva no desenvolvimento de novas dimensões para os direitos fundamentais: a superação da concepção de direitos fundamentais somente como direitos exigíveis em face do Estado, seja a uma *abstenção* (liberdades públicas), seja a uma *prestação* (sobretudo os direitos sociais). Direitos fundamentais, nesse novo paradigma, desempenhariam

[71] MOTTA, Sylvio. **Direito Constitucional.** 29. ed. Rio de Janeiro: Método, 2021, *E-Book*, p. 230, ISBN 9788530993993. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530993993/. Acesso em: 18 out. 2024.
[72] VALENTE, Manuel Monteiro. Os Direitos e Garantias dos cidadãos investigados na era digital. *In:*ANTONIALLI, Dennys; FRAGOSO, Nathalie (ed.). **Direitos Fundamentais e Processo Penal na Era Digital.** Doutrina e prática em debate, vol. 2., São Paulo: 2019, InternetLab, p. 25.
[73] Ibid., p. 26
[74] SILVA, Virgílio Afonso da. **A constitucionalização do direito** – os direitos fundamentais nas relações entre particulares. São Paulo: 2011, Editora Malheiros, p. 41.

> uma função adicional: eles expressariam um sistema de valores, válido para todo o ordenamento jurídico.
> Esse sistema de valores não pode ser confundido, contudo, com a superada ideia de "mera declaração de princípios" [...] A concepção de "declaração de princípios", muito difundida, especialmente na República de Weimar, quase sempre foi entendida como simples "declaração de intenções" do poder constituinte em relação à atividade legislativa, uma declaração sem valor normativo e, por isso, não-vinculante. Um sistema de valores pretende ser muito mais do que isso, pois é o ponto de partida, *vinculante*, para uma constitucionalização do direito e uma ampliação da própria força normativa da constituição [...][75].

Ao compreender esse sistema, a proteção dos dados deve se revelar num contexto não apenas de abstenção estatal, mas também em efetiva prestação positiva, no sentido de, ainda que dentro do âmbito de uma investigação criminal, sejam tomadas todas as cautelas para salvaguardar os interesses individuais.

Segundo Orlandindo Gleizer, "o direito processual penal, na busca de seus fins, intervém na esfera de direitos de uma série de pessoas", sendo que tais "intervenções colocam problemas que vão muito além do processo, que atinem já ao direito constitucional"[76].

Nesse sentido, é de rigor verificar as aplicações às relações entabuladas na *internet*, especialmente no que diz respeito à privacidade, não se perdendo de vista que nas interações que ocorrem na *internet*, existem características específicas que tornam a investigação do assunto integrada, isto é, não se pode avaliar cada um dos direitos de maneira isolada. Assim, o envio de mensagens não solicitadas por meios eletrônicos (*spam)* viola a privacidade e o sigilo de dados e, de outro lado, tem-se também a liberdade de expressão[77]. Isso traz à baila a própria questão da proporcionalidade quando existem conflitos entre direitos fundamentais:

> Desta forma, quando houver conflito entre dois ou mais direitos ou garantias fundamentais, o intérprete deverá utilizar-se do *princípio da concordância prática ou da harmonização*, de forma a coordenar e combinar os bens jurídicos em conflito, evitando o sacrifício total de uns em relação aos outros, realizando uma redução proporcional do âmbito de alcance de cada qual (*contradição dos princípios*), sempre em busca do verdadeiro significado da norma e da harmonia do texto constitucional com sua finalidade precípua [...][78].

---

[75] SILVA, Virgílio Afonso da. **A constitucionalização do direito** – os direitos fundamentais nas relações entre particulares. São Paulo: Editora Malheiros, 2011, p. 76-77.
[76] GLEIZE, Orlandino. **Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal.** Disponível em: https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-interv encoes-em-direitos-fundamentais-no-processo-penal-31072019. Acesso em: 20 ago. 2024.
[77] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 60.
[78] MORAES, Alexandre de. **Direito Constitucional**. 40. ed. Rio de Janeiro: Atlas, 2024. *E-book.* p. 92. ISBN 9786559776375. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559776375/. Acesso em: 18 out. 2024.

A questão se revela ainda mais sensível quando se trata de prova digital, que demanda conhecimentos específicos e, diante de seu caráter contemporâneo – à luz das evidências já existentes no ordenamento - vê-se a necessidade de compreender a matéria de provas dentro do âmbito penal, indo além, o que significa analisar todas as implicações que a *internet* traz em seu bojo. Dito por outras palavras, os benefícios são analisados junto com os malefícios. Isso denota que os estudos são viabilizados para ampliar o uso, ao mesmo tempo em que deve ser brecado perante a possíveis violações aos direitos e garantias consagrados. Não é, pois, tarefa fácil.

No que tange à investigação criminal, é certo que a tecnologia tem influenciado e facilitado significativamente suas práticas. Dessa forma, o crescente uso de dispositivos conectados à *internet*, juntamente com o surgimento de tecnologias de monitoramento, transformou a rotina das autoridades acerca da própria apuração em si, pois agora se deparam não apenas com novas fontes de evidência, mas também questões inéditas.

Muitas vezes as informações procuradas envolvem a área da intimidade ou privacidade pessoal do indivíduo, o que torna necessário avaliar a viabilidade de se apresentar a prova, considerando os direitos garantidos pela constituição. De maneira semelhante, a forma como a prova é realizada pode impor limitações a um direito ou garantia fundamental, como no caso da busca e apreensão de dispositivos eletrônicos, o que requer a entrada em residências e a restrição de direitos de propriedade. Assim, é relevante considerar a avaliação dessas evidências à luz da salvaguarda dos direitos fundamentais[79].

O contexto regulatório atual, embora não esteja totalmente desconectado dessas transformações, ainda apresenta desalinhamento em relação às inovações tecnológicas, o que pode levar a conflitos com direitos fundamentais e às garantias dos indivíduos.

Nesse novo contexto de amplas opções de repressão penal, o Estado pode acabar excedendo os limites constitucionais referentes à proteção da vida privada e à legalidade penal, enquanto avança lentamente na definição de critérios e mecanismos que assegurem a proteção desse núcleo fundamental de direitos[80].

Para ilustrar – e já adentrando na questão probatória digital -, pode-se destacar os dados de geolocalização, que envolvem a utilização de informações de localização para identificar a

---

[79] VAZ, Denise Provasi. **Provas Digitais no Processo Penal:** Formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade de São Paulo, São Paulo, 2012, p. 34.

[80] PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos**. São Paulo: 2014, Marcial Pons, p. 59.

presença de um determinado dispositivo ou pessoa em um local, podendo ser obtido por sinal de *internet* e GPS, sendo muito comum em dispositivos móveis e aplicativos, como o Waze[81].

Nesse sentido, é imperioso destacar a investigação do caso Marielle Franco, em que se discutiu acerca da possibilidade da plataforma Google fornecer a lista de usuários que realizaram pesquisas sobre a vereadora, assassinada em 14/03/2018. O caso, portanto, versa sobre a definição de limites para a quebra de sigilo de buscas na plataforma.

No caso, houve solicitação pelo Ministério Público da lista de usuários para identificar possíveis envolvidos no crime. A linha investigativa seguia a hipótese de que os autores do delito seguiam a vítima, sabendo, portanto, previamente que a vereadora estaria em determinado evento. Dessa forma, o intuito era identificar os Internet Protocols (IPs) que teriam utilizado o Google Maps ou Waze em determinado período anterior e no dia da morte para o endereço de destino em que a vereadora se encontrava, bem como quem teria realizado, no mesmo lapso temporal, parâmetros de pesquisa com seu nome.

Contudo, a plataforma Google alegou que a referida medida violaria a privacidade dos usuários, o que poderia abrir margem para que meras pesquisas se tornassem meios de vigiar, indevidamente, os cidadãos.

O C. Superior Tribunal de Justiça, no julgamento do RMS 61.302/RJ (Info 678), julgado em 26/08/2020, de Relatoria do Ministro Rogerio Schietti Cruz entendeu pela legalidade da medida, que não violaria princípios e garantias fundamentais. Isso porque o direito ao sigilo não possui dimensão absoluta, de tal sorte que é possível afastar sua proteção, se presentes situações que denotem "a existência de interesse público relevante, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução criminal"[82].

---

[81] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed. São Paulo: Revista dos Tribunais, 2024, p. 147.

[82] BRASIL. Superior Tribunal de Justiça. RMS 61302 / RJ, Relator Ministro Rogerio Schietti Cruz, Terceira Seção, julgado em 26/08/2020, DJe 04/09/2020. Consta do julgado, ainda que "4. A determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, as quais são acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. Há uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Decerto que o art. 5º, X, da CF/88 garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, o acesso a esses dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma". Acesso em: 10 jun. 2024.

Além disso, na referida decisão foi analisado outro princípio de suma importância, qual seja, a proporcionalidade, nos seguintes termos:

> [...] 10. Quanto à proporcionalidade da quebra de dados informáticos, ela é adequada, na medida em que serve como mais um instrumento que pode auxiliar na elucidação dos delitos, cuja investigação se arrasta por dois anos, sem que haja uma conclusão definitiva; é necessária, diante da complexidade do caso e da não evidência de outros meios não gravosos para se alcançarem os legítimos fins investigativos; e, por fim, é proporcional em sentido estrito, porque a restrição a direitos fundamentais que dela redundam – tendo como finalidade a apuração de crimes dolosos contra a vida, de repercussão internacional – não enseja gravame às pessoas eventualmente afetadas, as quais não terão seu sigilo de dados registrais publicizados, os quais, se não constatada sua conexão com o fato investigado, serão descartados.

Ora, observando-se outras medidas, a geolocalização pode revelar-se mais apropriada e proporcional, por ser menos invasiva. É evidente que todas as questões devem ser analisadas diante do caso concreto. Nesse sentido, não é possível a quebra de dados de geolocalização de pessoas indeterminadas, de modo abrangente e indiscriminado, afinal, uma das facetas do direito à privacidade é não ter suas informações exibidas a todos.

Acerca da proporcionalidade, Orlandino Gleizer ressalta que:

> [...] é uma relação entre a ação do Estado e os efeitos sobre o indivíduo: de um lado está o tamanho da intervenção na esfera individual e, do outro, a finalidade, a idoneidade, a necessidade e a adequação da medida para a produção do resultado pretendido (relação finalidade-meio), ou seja, se a finalidade da intervenção está em uma relação equilibrada com os danos sofridos pelo titular do direito. A subsidiariedade e a adequação, assim como todos os elementos dessa análise, também devem ser verificados em relação ao direito fundamental afetado, pois essa primeira barreira se impõe a qualquer ação estatal que afete a esfera protegida do indivíduo. A ausência de uma precisa estrutura lógico-dogmática de análise das intervenções em direitos fundamentais dificulta sobremaneira a reflexão dos aplicadores do direito e o próprio debate, que, sem essa estrutura, fica relegado a frases de efeito e argumentos desmontados[83].

A questão chegou ao Supremo Tribunal Federal (Tema 1148 – Limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas). Nesse sentido, no julgamento em 16/10/2024, o Ministro Alexandre de Moraes votou a favor da possibilidade da quebra de sigilo de dados de pessoas indeterminadas, desde que sejam "determináveis a partir de outros elementos de provas obtidos

[83] GLEIZE, Orlandino. Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal. **Jota,** 31 jul. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-31072019. Acesso em: 20 ago. 2024.

previamente na investigação e que justifiquem a medida". Além disso, é justificado em casos de crimes gravíssimos:

> 1) É constitucional a requisição judicial de registros de conexão ou de registros de acesso a aplicações de internet para fins de investigação criminal ou instrução processual penal, desde que observados os requisitos previstos no artigo 22 da Lei 12.965/2014 (Marco Civil da Internet), quais sejam: (a) fundados indícios de ocorrência do ilícito; (b) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; (c) período ao qual se referem os registros.
> 2) A ordem judicial poderá atingir pessoas indeterminadas, desde que determináveis a partir de outros elementos de prova obtidos previamente na investigação e que justifiquem a medida[84].

Vê-se, portanto, que não é tarefa fácil, tampouco sem debates que vão além das normas estabelecidas no ordenamento jurídico, afinal, o processo penal aponta o embate entre o dever-poder de punir e o direito do investigado na defesa de suas liberdades. Logicamente, a ponderação se fará presente.

Nesse sentido, o STJ, no julgamento do RMS 68119-RJ, julgado em 15/03/2022 (Info 730), de relatoria do Ministro Jesuíno Rissato, entendendo que não é possível que se determine a quebra em um universo indefinido de indivíduos quando as informações incluírem dados de pessoais sensíveis (como o acesso total a imagens e diálogos). Assim constou:

> Em regra, é possível que o juiz determine a quebra de sigilo de dados informáticos estáticos (registros), relacionados à identificação de usuários que operaram em determinada área geográfica, suficientemente fundamentada. Isso não ofende a proteção constitucional à privacidade e à intimidade. Ex: determinação ao Google a identificação dos IPs ou Device Ids que tenham se utilizado do Google Maps e/ou do Waze no dia do crime, no período das 19h até as 23h, para realizar consulta do endereço onde ocorreu o delito. Isso é, em tese, válido.
> No entanto, não é possível que se determine a quebra de sigilo de um universo indeterminado de pessoas quando os dados envolverem informações íntimas (como o acesso irrestrito a fotos e conteúdo de conversas).
> Assim, será inválida a ordem se o juiz determinou que o Google fornecesse o acesso aos seguintes dados das pessoas que estiveram no local: conteúdo dos e-mails do Gmail; conteúdo do Google Fotos e do Google Drive; listas de contatos; históricos de localização, incluindo os trajetos pesquisados; pesquisas feitas no Google; e listas de aplicativos baixados[85].

---

[84] NUNES, Vinícius. Moraes vota a favor de quebra de sigilo de dados de pessoas indeterminadas. **Jota,** 16 out. 2024. Disponível em: https://www.jota.info/stf/do-supremo/moraes-vota-a-favor-de-quebra-de-sigilo-de-dados-de-pessoas-indeterminadas. Acesso em: 19 out. 2024.

[85] Não é possível a quebra de sigilo de dados informáticos estáticos (registros de geolocalização) nos casos em que haja a possibilidade de violação da intimidade e vida privada de pessoas não diretamente relacionadas à investigação criminal - Buscador Dizer o Direito. Ainda, constou: "Não é necessário que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação, tampouco que justifique a indispensabilidade da medida, ou seja, que a prova da infração não pode ser realizada por outros meios [...] No caso concreto, contudo, a ordem foi bem mais ampla [...] O Poder Judiciário não deve determinar a quebra de sigilo de dados informáticos estáticos obtidos por registros de geolocalização do Google nos casos em que há a possibilidade de violação da intimidade e da vida privada de um número indeterminado de pessoas, que podem sequer estar relacionadas à

Além disso, no campo de proteção também se encontra a questão do sigilo da correspondência e das comunicações telegráficas, nos termos do art. 5º, inciso XII da CF/88, que estabelece ser "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".

Nesse sentido, vale mencionar o caso Prosegur, que ocorreu em Ribeirão Preto/SP, ocasião em que o juiz solicitou dados das contas de celular ao Google, Apple e Microsoft em determinado raio e período, além do "Internet Protocol (IP) dos aparelhos telefônicos, data e hora dos acessos (logins), marca e modelo dos celulares, número telefônico do dispositivo, as fotos armazenadas nos últimos 30 dias no Google Fotos [...] e todas as senhas armazenadas no serviço passwords.google.com"[86]. Neste caso, há quem entenda pela ilicitude da prova, por lesão a direito fundamental, pois "a invasão remota e oculta na privada esfera virtual do indivíduo representa uma intervenção mais severa e de natureza distinta", não sendo permitido ao juiz "ultrapassar os limites estabelecidos pelo legislador para afetação do âmbito de proteção de um direito fundamental"[87].

Acerca do conflito e harmonização de direitos, Tarcísio Teixeira menciona que:

> [...] torna-se evidente a necessidade de se buscar um equilíbrio para o exercício dos direitos previstos na Constituição, tendo em vista as relações estabelecidas na internet, notadamente quanto aos direitos da liberdade de expressão, da privacidade e do sigilo das correspondências, das comunicações e dos dados. Um caminho para isso é deixar claro que eles serão relativizados a fim de assegurar o interesse coletivo sobre o interesse individual. Esse é, não de modo exclusivo, mas principalmente, um dos papeis da jurisprudência[88].

O que se denota dos julgados acima colacionados é que, no âmago de combater a criminalidade, a adoção de métodos invasivos pode acabar sendo necessária, porém, em

---

investigação criminal" (CAVALCANTE, Márcio André Lopes. Não é possível a quebra de sigilo de dados informáticos estáticos (registros de geolocalização) nos casos em que haja a possibilidade de violação da intimidade e vida privada de pessoas não diretamente relacionadas à investigação criminal. **Buscador Dizer o Direito,** Manaus. Disponível em: https://buscadordizerodireito.com.br/jurisprudencia/detalhes/35ec253885cf090f80881b44180afb00. Acesso em: 12 out. 2024).

[86] COURA, Kalleo; LEORATTI, Alexandre**.** Juízes ordenam quebra de sigilo de sigilo com base em localização. **Jota,** 27 maio 2019. Disponível em: https://www.jota.info/especiais/juizes-ordenam-quebra-coletiva-de-sigilo-de-dados-com-base-em-localizacao 27052019. Acesso em: 7 jul. 2024.

[87] GLEIZE, Orlandino. Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal. **Jota,** 31 jul. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-31072019. Acesso em: 20 ago. 2024.

[88] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 69.

contrapartida, pode ir na contramão dos já consagrados direitos. Daí o debate acerca da necessidade de diploma específico quanto às provas digitais e suas possibilidades investigativas.

A individualização e identificação quanto às buscas pessoais é debatido inclusive no STF, na Repercussão Geral do tema 1148[89] (*Leading case* 1301250), de relatoria da Ministra Rosa Weber:

> 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.

No âmbito da investigação criminal, a Lei º 13.344/2016 inseriu dispositivos no Código de Processo Penal, estabelecendo que nos crimes de sequestro e cárcere privado, redução à condição análoga à de escravo, tráfico de pessoas, extorsão mediante sequestro e promoção ou auxílio para envio de criança ou adolescente para o exterior, com o fim de obter lucro, o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do Poder Público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeito (art. 13-A). Além disso, se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, que também podem requisitar, mas mediante autorização judicial, às empresas prestadoras de serviço de telecomunicação e/ou telemática, que disponibilizem meios adequados para localização da vítima ou dos suspeitos (art. 13-B).

A Associação Nacional das Operadoras Celulares (ACEL) ajuizou ADI para impugnar tais dispositivos, ao fundamento de que a previsão afrontaria os incisos X e XII do art. 5º, da CF/88, além de não guardar proporcionalidade, haja vista a possibilidade de quebra de dados em hipóteses genéricas. No entanto, tais dispositivos foram considerados constitucionais, pelo STF, no julgamento da ADI 5.642/DF, em 19/04/2024, de relatoria do Ministro Edson Fachin (Info 1133).

---

[89] Tema 1148: "Limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas".

Dessa forma, o direito à privacidade não é total, mas sim qualificado, o que implica dizer que a legislação pode limitar esse direito ao estabelecer situações em que o Judiciário pode suspendê-lo, sendo a razão para essa limitação permitir a investigação de violações da lei, uma vez que as evidências de tais infrações geralmente não estão acessíveis ao público. Dessa forma, deve-se considerar a flexibilização da proteção constitucional à privacidade e à vida pessoal em prol do interesse coletivo de elucidar esses delitos, uma vez que exigem rapidez nas investigações, especialmente para salvar as vítimas. Além disso, as normas que foram questionadas não oferecem um poder excessivo de solicitação, mas apenas o que é essencial para coibir infrações graves que ameaçam a liberdade individual e que visam possibilitar o resgate das vítimas enquanto os crimes ainda estão ocorrendo[90].

Aliás, nesse sentido, a Lei de Lavagem de Dinheiro estabelece que:

> A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informem qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito (art. 17-B da Lei nº 9.613/98, incluído pela Lei nº 12.683/2012) [e, ainda, a Lei de Organizações Criminais, em que] O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito (art. 15 da Lei nº 12.850/2013).

Aliás, o § 1º do art. 10-A da Lei nº 12.850/2013, incluído pelo Pacote Anticrime (Lei nº 13.964/2019), estabelece que dados cadastrais são "informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão".

Objetivando estabelecer princípios, garantias e deveres para o uso da *internet* no Brasil, bem como as diretrizes para atuação, em 2014 foi editada a Lei nº 12.965, conhecida como o Marco Civil da Internet (MCI); posteriormente, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, estabelecendo novo paradigma no tratamento de dados pessoais.

Mais à frente, a proteção foi alçada como direito fundamental (art. 5º, LXXIX, CF/88).

O que se vê, portanto, é a necessidade de os direitos constitucionais encontrarem harmonia com o novo contexto trazido pela *internet*, hoje com (quase) completa fusão entre o

---

[90] CAVALCANTE, Márcio André Lopes. São constitucionais os arts. 13-A e 13-B do CPP, inseridos pela Lei 13.344/2016**.** **Buscador Dizer o Direito**, Manaus. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/8e86a13d18f6dcab5a77f0a4525c0b20. Acesso em: 18 out. 2024.

homem e os dispositivos digitais, haja vista que a maior parte das relações ocorre por meio de sítios eletrônicos e aplicativos.

É fato: as pessoas estão todas conectadas. Até mesmo o sono é monitorado por meio do celular; prontuários médicos são mantidos na rede. Estes são apenas alguns dos (muitos) exemplos que denotam a necessidade de proteção ao acesso de forma a balizar sua utilização sem retrocesso aos direitos e garantias fundamentais e, ao mesmo tempo, que não impeçam a investigação penal. É função primordial do operador do direito, que lida com lacunas, trabalhar com tais provas de modo a interpretar dentro dessa sistemática, que ainda se revela um território novo.

No presente cenário social, caracterizado pela sociedade da informação, os dados pessoais passaram inclusive a ser considerados valiosos recursos na própria economia digital. Como já dito, informações individuais são frequentemente compartilhadas (especialmente em redes sociais), o que leva a uma exposição significativa desses dados que, em um contexto mais analógico, seriam sobremaneira mais difíceis de se obter.

Portanto, na era digital, a defesa dos direitos de personalidade é extremamente relevante, pois eles são os elementos que distinguem cada indivíduo dentro da coletividade. Transmudando o tema para a prova digital dentro do processo penal, tal possibilidade se revela imperiosa, diante da liberdade de locomoção que está em jogo.

2.2 O SIGILO DE DADOS NA *INTERNET* E SUA PROTEÇÃO CONSTITUCIONAL

Como já se viu, a proteção de dados foi alçada a status de direito fundamental na Constituição Federal, por meio da Emenda Constitucional nº 115/2022, assegurando a "proteção dos dados pessoais, inclusive nos meios digitais" (art. 5º, LXXIX, CF/88).

Foi, portanto, erigido à condição de cláusula pétrea (art. 60, § 4º, IV, CF/88), de modo que não pode ser abolido nem sequer por meio de emenda constitucional. Isso significa que não há a possibilidade de ato infraconstitucional violar tal direito. Por essa razão, qualquer legislação que trate sobre o tema, deve levar em consideração essas balizas constitucionais.

Nesse sentido, os dados fiscais e bancários, que estão registrados tanto nas instituições financeiras quanto na Receita Federal ou em entidades similares do governo, fazem parte da

vida privada do indivíduo ou da empresa, daí a necessidade do endosso do Poder Judiciário para a quebra[91].

Mais do que isso: ao proteger o sigilo de dados, não se tutela apenas a reserva quanto às informações privadas de pessoas físicas e jurídicas, mas o dever daqueles que detêm seu domínio de proteção e zelo em qualquer divulgação. Isso ganha relevo quando se trata das provas digitais e dados em nuvem.

Nesse sentido, o STF decidiu que "os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida", de modo que "toda e qualquer decisão de fornecimento desses dados deverá ser devida e formalmente motivada para eventual controle de legalidade pelo Poder Judiciário"[92].

Tarcísio Teixeira destaca:

> Sobre a expressão "direito fundamental", o qualitativo "fundamental" serve para diferenciar o grau de importância de um direito ao ser comparado com outros; portanto, direitos fundamentais são tidos por sagrados, mais relevantes. Sendo assim, com a inclusão da proteção de dados como direito fundamental previsto na Constituição Federal, ele passa a estar alinhado em grau de importância com outros direitos sagrados, como a vida, liberdade, segurança, entre outros.
> [...]
> Ao elevar a proteção de dados a um patamar mais valioso no ordenamento jurídico, o constituinte derivado declarou que esse direito deve ser respeitado de maneira ainda mais rigorosa, o que contribui simbolicamente para sua efetividade (ou eficácia social). Significa dizer que, na prática, a nova previsão não altera o conteúdo dos projetos de adequação à LGPD, por exemplo, mas eleva a relevância que o Estado, o mercado e os cidadãos darão à existência ou não de adequação em determinadas instituições e empresas [...][93].

E aqui encontra-se um ponto fulcral de debate. O supracitado artigo, como se viu, resguarda o sigilo de dados, mas encontra, na prática, um possível obstáculo: a investigação criminal e os meios de obtenção de prova.

Ora, considerando que tais dados se encontram muitas vezes dispostos em nuvem (como no caso outrora citado, em que foi determinado o acesso ao Google Fotos[94]), o caminho às

---

[91] MORAES, Alexandre de. **Direito Constitucional**. 40. ed. Rio de Janeiro: Atlas, 2024. *E-book.* p.92. ISBN 9786559776375. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559776375/. Acesso em: 18 out. 2024.

[92] BRASIL. Supremo Tribunal Federal. **ADI 6529/DF**, Rel. Min. Cármen Lúcia, julgamento virtual finalizado em 8/10/2021.

[93] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 75-77.

[94] COURA, Kalleo; LEORATTI, Alexandre**.** Juízes ordenam quebra de sigilo de sigilo com base em localização. **Jota,** 27 maio 2019. Disponível em: https://www.jota.info/especiais/juizes-ordenam-quebra-coletiva-de-sigilo-de-dados-com-base-em-localizacao 27052019. Acesso em: 7 jul. 2024.

informações pode se encontrar em um cenário nebuloso em que o amplo acesso é permitido ou não.

Dessa forma, ao realizar a coleta e análise de evidências, é fundamental garantir o respeito aos direitos das pessoas, evitando a divulgação de dados pessoais sensíveis que não sejam pertinentes ao caso que está sendo investigado. A proteção da privacidade dos indivíduos deve ser mantida, exceto quando houver uma razão legal adequada e uma determinação judicial que autorize a divulgação de informações específicas.

O legislador, como se viu nos dispositivos 13-A e 13-B do CPP, vem caminhando nesse sentido, pois encontra-se evidenciada a necessidade de adequação dos diplomas normativos atuais às exigências da sociedade frente à tecnologia.

A adoção de técnicas sofisticadas para a coleta e a análise de provas digitais levanta questões éticas relevantes pois a captura de informações eletrônicas pode acarretar violações de privacidade, especialmente em relação a aparelhos pessoais – afinal, não há dúvida de que a "vida" de alguém pode ser facilmente encontrada em seu smartphone.

A mudança de paradigmas ocorre numa velocidade que, de certo, o ordenamento jurídico – mais precisamente as normas processuais penais – não conseguem alcançar. Em outras palavras, novos meios de investigação surgem em um ritmo muito mais rápido do que as leis são promulgadas.

Daí porque o debate quanto à possibilidade de acesso e como isso poderia violar os supedâneos constitucionais revela-se imprescindível hodiernamente. De outro modo, a regulação não pode configurar censura ou licença, também vedado pelo texto constitucional.

Thomas Law assim entende:

> No estágio atual do mundo, a sociedade possui uma nova forma de organização em que a informação é o elemento nuclear para o desenvolvimento da economia. A sociedade informacional manifesta-se pelo incremento permanente de novas tecnologias, pela globalização intensa, pela rapidez das comunicações e por mudanças comportamentais. Após a Revolução Agrícola e a Revolução Industrial, **vivenciamos a Revolução Digital**, em que a informação, o conhecimento e a alta tecnologia são modalidades de capital fundamentais para o mercado contemporâneo [...] atualmente existe uma difusão dos meios de interação no contexto do ciberespaço, este enquanto um ambiente de participação e relacionamento entre atos públicos e privados[95] (grifos nossos).

[95] LAW, Thomas. **A Lei Geral de Proteção de Dados – LGPD.** Uma análise comparada ao novo modelo chinês. São Paulo: D'Plácido, 2021, p. 31-32.

Como já mencionado, a privacidade está associada ao que é reservado, com acesso limitado, diferentemente do público, que é amplamente conhecido[96]. Entender a privacidade dentro da perspectiva digital é, acima de tudo, ponderar a necessidade de sua ampliação, porque é justamente isso que a *internet* possibilita e faz: ao mesmo tempo em que é um mecanismo necessário e eficiente para a salvaguarda de dados (antes, um cenário em que toneladas de arquivos em papel que podem, inclusive, desaparecer) para as mídias (como *cloud system*), mas que poderiam, ao mesmo tempo, colocar em risco a privacidade, justamente diante da facilidade de acesso.

Não é preciso ir longe. Hoje, em pesquisa rápida pelo próprio nome no Google é possível obter diversas informações em que, muitas das vezes, o próprio detentor sequer teve acesso ou controle. Indo além, como saber se não se está sendo observado ou até mesmo vigiado? O mundo está, atualmente, num emaranhado complexo hiperconectado, daí porque essa perspectiva orwelliana[97] não é exagerada. Conforme Bomfati e Kolbe:

> A verdade é que as tecnologias modernas permitem que um cidadão seja espionado de inúmeras formas diferentes, sem que ele saiba. Os aparelhos de televisão fabricados atualmente chamam-se *smart TV*, porque juntam televisão com internet. Assim, caso esteja conectado à internet, não seria possível que o fabricante de TV tivesse algum dispositivo implantado nela que possibilitasse a ele visualizar ou ouvir o usuário enquanto ele assiste a um jogo de futebol, por exemplo? Ou, ainda, será que um *Homo sapiens hacker* não seria capaz de invadir essa TV e implantar um dispositivo espião? Ora, não sejamos ingênuos. É óbvio que existe tecnologia para isso, da mesma forma que um dispositivo espião pode fazer com que a câmera do *smartphone* ou do computador seja ligada sem percebermos, é possível que a *smart TV* seja mais esperta do que pensamos [...][98].

As maravilhas que a tecnologia proporciona são as mesmas que podem também causar problemas. Atualmente, para ter uma conta em algum banco basta acesso à *internet.* No entanto, fato é que nunca se saberá ao certo quem tem acesso a todo o sistema. Tanto é verdade que inúmeros indivíduos têm seus dados disponibilizados com contas bancárias que nem sequer têm conhecimento.

A fusão entre ser humano-internet já está enraizada, estando implícita no momento do aceite aos termos do sítio eletrônico sem que se saiba ao certo em quais mazelas isso poderia implicar.

---

[96] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 55.

[97] Relativo a George Orwell (1903-1950), escritor inglês, à sua obra ou ao seu estilo. ORWELLIANA. *In:* **PRIBERAM**, Dicionário Priberam da Língua Portuguesa. Disponível em: https://dicionario.priberam.org/orwelliana. Acesso em: 10 jul. 2024.

[98] BOMFATI, Cláudio Adriano; KOLBE, Armando Júnior. **Crimes cibernéticos**. 1ª ed. Curibita: Intersaberes, 2020, p. 73-74

Tais fatores englobam amplo conjunto de operações que podem ocorrer em meios manuais ou digitais, razão pela qual existe um desafio regulatório, na medida em que a questão da privacidade e a proteção de dados contém elementos particulares que necessitam de revisão dos marcos de atuação de entes públicos e privados, uma vez que os paradigmas não guardam profunda identidade entre o que se vivencia enquanto vida particular no mundo real e o que se tem no universo virtual. A questão é: até quando? Afinal, o metaverso, ambiente que combina realidade física e virtual, já existe. Como serão tutelados esses direitos? O operador do direito está pronto para atuar diante desse prisma?

Nesse cenário, surge a necessidade de proteção desses dados, com vistas também à segurança da informação que, como já dito, ganhou status de direito fundamental autônomo.

Todo tipo de tecnologia e serviço que gera e transmite dados, além de documentar fatos, são de interesse para o Estado e órgãos de investigação. E é certo que muitos desses registros são pessoais e é este o ponto de partida de discussão, com articulações inovadoras acerca da privacidade, pois nenhum direito é absoluto.

É legítimo, afinal, que a autoridade policial, por exemplo, tenha interesse na construção de um arcabouço probatório para eventualmente punir aquele que comete ou pratique conduta ilícita. Contudo, existem diversas questões pendentes e que têm desafiado as doutrinas subjacentes a todo esse panorama jurídico.

Nesse sentido, Antonialli e Fragoso discorrem que:

> Ao provocar uma transformação na forma como as pessoas se comunicam, possibilitando a substituição das chamadas telefônicas tradicionais por aplicações de mensagens instantâneas, e-mails e até chamadas de voz sobre IP habilitadas para web, os telefones celulares também se tornaram um tesouro de informações de comunicações, particularmente para autoridades de segurança pública. Além dos registros detalhados sobre quando, onde e por quanto tempo as comunicações ocorreram, essas novas formas de troca de informações também podem armazenar todo esse conteúdo e muito mais, como lista de contatos, fotos, notas, listas de leitura, histórico de páginas visitas, dados de localização[99].

Portanto, a discussão sobre a incorporação da tecnologia ao sistema processual penal reflete as necessidades de uma sociedade que passou por transformações. Os efeitos da informação – da Revolução Digital – sinalizam um rumo irreversível nas estruturas das investigações de crimes.

Dessa forma, se a abordagem de repressão à criminalidade e investigação se alteram, os meios de prova relacionados também assim seguirão, daí porque, como será analisado adiante,

---

[99] ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital:** Doutrina e Prática em Debate. v. 2. São Paulo. Internet Lab, 2019, p. 62.

o estudo da coleta de provas digitais, cadeia de custódia e todas as inquietudes que o tema tem no seu escopo, é imprescindível.

2.3 MARCO CIVIL DA INTERNET - LEI 12.965/14

Objetivando estabelecer princípios, garantias e deveres para o uso da *internet* no Brasil, bem como deliminar diretrizes na atuação, em 2014 foi editada a Lei nº 12.965, conhecida como o Marco Civil da Internet, revelando-se como verdadeiro microssistema de proteção aos usuários da *internet*, encarando as questões jurídicas latentes que se puseram à disposição diante dos imbróglios já presentes e que, sem dúvidas (e como ainda se pode observar), só cresceriam.

Referido diploma, além de regulamentar a atividade, assegura o sigilo de dados (art. 7º) e traz novos panoramas em relação à privacidade, com uma série de princípios que visam transparência e limitação, havendo preocupação em relação às condições de coleta e armazenamento de dados.

Dessa forma, a positivação de certas questões se fez indispensável, considerando que o progresso tecnológico levou ao surgimento de situações que não eram abordadas de maneira clara pelo sistema jurídico, o que possibilitou diversas interpretações[100].

Segundo Bomfati e Kolbe:

> A rapidez do avanço tecnológico trouxe aos indivíduos uma fama enorme de formas de agir dentro de uma sociedade e, por consequência, exigiu do direito uma nova linha de pensar e atuar, de modo que se adaptasse a essa nova realidade. Ou seja, para além das questões criminais, existe uma série de outras atividades praticadas pela internet, partindo da compra e venda de produtos, até o trabalho que pode ser desenvolvido dentro de casa, tudo precisando ser regulamentado.
> Assim, surgiu o direito digital, que busca a regularização desse mundo tecnológico, definindo direitos e deveres. Para tanto, surgiu a ideia do Marco Civil da Internet, que trata da construção dos cidadãos dessa rede, ou seja, não se fala apenas de crimes na internet, mas de tudo o que for necessário ser discutido e regulamentado em todas as áreas em que a tecnologia da informação se faça presente[101].

O Marco Civil da Internet trata dos "princípios, garantias, direitos e deveres para o uso da internet no Brasil" (art. 1º), determinando suas diretrizes, sendo "marco" porque é referência, demarcação dos direitos dos cidadãos em relação ao uso da rede mundial de computadores[102].

---

[100] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 104.
[101] BOMFATI, Cláudio Adriano; KOLBE, Armando Júnior. **Crimes cibernéticos**. Curibita: Intersaberes, 2020, p. 66-67.
[102] TEIXEIRA, op. cit., p. 84.

Referido diploma foi promulgado visando proteger os direitos fundamentais de liberdade, privacidade e liberdade de expressão, bem como o livre desenvolvimento da personalidade dos indivíduos por meio da promoção de uma cultura de proteção de dados (pessoais), dispostos em meio físico ou digital, tanto que foi apelidado de "Constituição da Internet".

A liberdade de expressão (direito fundamental que consiste na faculdade de todos os cidadãos poderem exprimir e divulgar seus pensamentos) é um dos fundamentos assegurados pela MCI, estabelecendo: (i) reconhecimento da escala mundial da rede; (ii) os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; (iii) a pluralidade e a diversidade; (iv) a abertura e a colaboração; (v) a livre iniciativa, a livre concorrência e a defesa do consumidor; e (vi) a finalidade social da rede (art. 2º).

É diploma principiológico, garantindo: (i) liberdade de expressão, comunicação e manifestação de pensamento; (ii) proteção da privacidade; (iii) proteção dos dados pessoais; (iv) preservação e garantia da neutralidade de rede; (v) preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; (vi) responsabilização dos agentes de acordo com suas atividades; (vii) preservação da natureza participativa da rede; e (viii) liberdade dos modelos de negócios promovidos na *internet*, desde que não conflitem com os demais princípios (art. 3º).

É importante frisar que no cenário internacional houve a edição da Carta de Direitos Humanos e Princípios para a Internet que, em 2024, trouxe a discussão acerca do impacto da Inteligência Artificial[103], o que denota que as questões atinentes ao acesso à rede mundial de computadores e suas transformações continuam sendo objeto de estudo e debate.

Como objetivos do MCI estão: (i) direito de acesso à internet a todos; (ii) acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos; (iii) inovação e fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e (iv) adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados (art. 4º).

Aliás, é expressamente previsto ainda que, na interpretação, devem ser "levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural" (art. 6º).

---

[103] INTERNET RIGHTS AND PRINCIPLES DYNAMIC COALITION. Promoting human rights as digital rights. **IRPC,** 19 jun. 2024. Disponível em https://internetrightsandprinciples.org/. Acesso em: 12 out. 2024.

O art. 5º, inc. I da Lei define internet como "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes".

Em relação aos direitos e garantias dos usuários, são assegurados: (i) a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; (ii) inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; (iii) inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; (iv) não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; (v) manutenção da qualidade contratada da conexão à internet; e (vi) informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade (art. 7º).

Também estabelece a proteção quando trata da possibilidade de exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas na Lei e naquela que dispõe sobre a proteção de dados pessoais; publicidade e clareza de eventuais políticas de uso dos provedores de conexão e aplicação de internet; acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet (art. 7º, incisos X, XI, XII e XIII, respectivamente).

Acerca da captação e formação de banco de dados, com consequente cessão e comercialização para terceiro, a lei destaca que serão asseguradas informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicação de internet. Ainda, trata do consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (art. 7º, incisos VIII e IX, respectivamente).

Também é direito do usuário de internet o não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (art. 7º, inciso VII).

Tarcísio Teixeira ressalta, acerca do MCI, que:

> [...] a norma segue o padrão europeu e argentino quanto à necessidade de autorização expressa do usuário para a coleta de dados, bem como para o seu uso, armazenamento e tratamento de dados pessoais, não podendo ser fornecidos a terceiros, salvo consentimento. Assim, Europa e Argentina adotam o sistema *opt-in*. Ao contrário, os Estados Unidos seguem sistema *opt-out*, em que se podem utilizar os dados livremente independente de prévio consentimento; mas se o usuário solicitar a exclusão de seus dados e/ou não envio de mensagens e, ainda assim, o remetente insiste, isso é considerado crime[104].

Vê-se, portanto, uma preocupação na MCI com a garantia do direito à privacidade e liberdade de expressão, de modo que são nulas as cláusulas contratuais que violem tais pontos, como aquelas que "impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet" ou "em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil" (art. 8º, caput e parágrafo único).

O art. 9º trata da neutralidade de rede; nesse sentido, o "responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, terminal ou aplicação".

Em outras palavras, o tráfego de internet deve ser realizado de forma igualitária, sem restrições, discriminação ou interferências, de modo que se o usuário deseja acesso para enviar e-mail ou acessar determinado sítio eletrônico, não pode haver privilégios ou prejuízos, devendo ocorrer de forma livre. A diferenciação somente será possível em casos de "requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações" e "priorização de serviços de emergência", sendo devidamente regulamentada nos termos das atribuições privativas do Presidente da República, ouvidos o Comitê Gestor da Internet (CGI), e a Agência Nacional de Telecomunicações (Anatel) (art. 9º, § 1º, incisos I e II), tudo realizado com "proporcionalidade, transparência e isonomia", além de "informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede" e "oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais" (art. 9º, § 2º, inciso II, III e IV).

No mais, "na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados" (art. 9, § 3º).

Conforme Carlos Affonso Souza e Ronaldo Lemos:

---

[104] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 92.

> Neutralidade significa manter as regras de tráfego estabelecidas pelos padrões que regem a própria internet como um todo, evitando assim que operadores de trechos da rede possam ditar suas próprias regras extravagantes[105].

No que tange à proteção aos registros e dados, a lei estabelece, em consonância com os ditames constitucionais, que o conteúdo deve atender à "preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas" (art. 10), de modo que apenas por meio de ordem judicial o provedor será obrigado a disponibilizar os registros (art. 10, §§ 1º e 2º).

A coleta, armazenamento, guarda e tratamento de registros e dados em que ao menos um dos atos ocorra no território nacional, devem respeitar a legislação brasileira (art. 11, caput e § 1º), o mesmo em relação às atividades que sejam realizadas por pessoa jurídica sediada no exterior, mas oferte serviço ao público brasileiro ou grupo econômico que possua estabelecimento no Brasil (art. 11, § 4º).

O MCI estabelece sanções caso haja o descumprimento das disposições previstas nos artigos 10 e 11, sem prejuízo das cíveis, criminais ou administrativas, a saber: (i) advertência, com indicação de prazo para adoção de medidas corretivas; (ii) multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; (iii) suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou (iv) proibição de exercício das atividades que envolvam os atos previsto no art. 11 (art. 12, caput). Além disso, tratando-se de empresa estrangeira, haveria a responsabilidade solidária pelo pagamento da multa (art. 12, parágrafo único).

Já o art. 13 da Lei determina o dever de manter os registros de conexão (IPs, hora de acesso, etc.), sob sigilo e em ambiente controlado, pelo prazo de um ano, período que pode ser estendido caso haja requerimento da autoridade policial, administrativa ou do Ministério Público (art. 13, § 2º), sendo que a disponibilização sempre deverá ser precedida de autorização judicial (art. 13, § 4º). Além disso, a autoridade requerente tem o prazo de 60 dias, contados a partir do requerimento, para ingressar com pedido de autorização de acesso (art. 13, § 3º).

Nesse ponto, é importante destacar o entendimento do STF, no HC 222.141 AgR/PR, de relatoria do Ministro Ricardo Lewandovsky, julgado em 06/02/2024 (Info 1123), que

---

[105] SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco Civil da Internet:** construção e aplicação. Juiz de Fora: Editar Editora Associada, 2016, p. 116.

entendeu que as provas obtidas a partir de dados preservados em contas da internet sem prévia autorização judicial de quebra de sigilo e fora das hipóteses legais, são nulas.

No caso em comento, o Ministério Público do Paraná, durante investigação relacionada à irregularidade quanto ao credenciamento de empresas para serviços de registro eletrônico de contratos, realizou pedido às plataformas Apple e Google para que mantivessem os dados e os IMEIs (identificação de equipamento móvel) associados às contas de um dos sócios das empresas investigadas. O pleito englobava dados cadastrais, histórico de localizações, pesquisas e conteúdos de e-mails, mensagens e fotos.

Impetrado *habeas corpus*, em que a defesa afirmava que a coleta das evidências teria infringido o direito à privacidade e intimidade, contrariando as diretrizes estabelecidas pelo MCI. Assim constou do julgado:

> [...] o supracitado pedido formulado pelo *Parquet* não teve lastro em qualquer decisão judicial de quebra de sigilo telemático, muito embora, a rigor, isso significasse impedir a disponibilidade, por parte da investigada, de todos os dados que estivessem armazenados nas referidas plataformas, a contar do dia 1º/6/2017 até a data do requerimento. O pedido de quebra do sigilo da paciente, em verdade, foi apresentado à autoridade judicial somente em 29/11/2019, tendo o juízo singular deferido fundamentadamente o pleito em 3/12/2019 [...]
> Assim, o ponto nodal da discussão consiste em saber se o "congelamento" – e consequente perda da disponibilidade – de todo o conteúdo de *e-mails*, mensagens, contatos e históricos de localização da paciente encontra-se albergado pela reserva de jurisdição, à vista do direito à preservação da intimidade, da vida privada, da honra e da imagem das pessoas (art. 5º, X, da Constituição Federal). Anoto, outrossim, que o inciso XII do Texto Maior igualmente estatui que "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".
> A jurisprudência desta Suprema Corte tem afirmado reiteradamente que o inciso XII do art. 5º da Carta Magna protege o sigilo das comunicações em fluxo (troca de dados e mensagens). Assenta também que o sigilo das comunicações armazenadas, como depósito registral, é tutelado pela previsão constitucional do direito à privacidade, na forma do inciso X do art. 5º, CF (cito, *v.g.*, o HC 91.867/PA, relator Ministro Gilmar Mendes). No campo infraconstitucional, o Marco Civil da Internet (Lei 12.965/2014) traça os princípios aplicáveis em nosso ordenamento, enumerados no art. 3º, tal como o da proteção da privacidade e dos dados pessoais, assegurando, outrossim, a inviolabilidade e sigilo do fluxo de suas comunicações privadas armazenadas, ressalvada ordem judicial de sua quebra (art. 7º da mencionada lei).
> Partindo dessas premissas, tenho que o pedido de indisponibilidade dos registros de que trata a Lei 12.965/2014 (dados intercambiados), seja pelo Ministério Público, seja por autoridades policiais ou administrativas, em atenção à referida cláusula constitucional, deverá, a toda evidência, ser precedida de indispensável autorização judicial. Sim, pois, na forma do art. 5º, V, da supracitada legislação, os registros de conexão se referem, tão somente, ao conjunto de informações concernentes à data e hora de início e de término de uma conexão à internet, sua duração e o endereço de IP utilizado pelo terminal. Registros de acesso a aplicações de internet, por sua vez, previstos no inciso VIII do citado dispositivo, tratam apenas do conjunto de informações relativas à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço de IP.
> [...]

> A referida legislação, no art. 10, § 1º, ao tratar de forma específica da proteção aos registros, dados pessoais e comunicações privadas, é clara quanto à possibilidade de fornecimento de informações de acesso (registro de conexão e registro de acesso a aplicações de internet), **desde que sejam requisitados por ordem de um juiz**.
> [...]
> Já a subseção I do mesmo texto cuida da "Da Guarda de Registro de Conexão" [...]
> Verifica-se que a autoridade requerente tem 60 dias para pleitear o acesso aos registros de conexão, quais sejam, tão somente 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. Tais elementos, portanto, não se confundem com o material telemático, como, por exemplo, o conteúdo de *e-mail, iMessagens/hangouts*, fotos e contatos.
> Caso prevalecesse o entendimento esposado no acórdão combatido, toda e qualquer autoridade policial ou o próprio Ministério Público poderiam requisitar aos provedores da internet, sem a devida autorização, a indisponibilidade de dados telemáticos de qualquer investigado, situação que, a toda evidência, não se concede. Nesta senda, rememoro as palavras do Ministro Edson Fachin no julgamento da ADPF 403/DF, de sua relatoria, ao enfatizar que a privacidade é o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública [...]
> Assim, vê-se que cabe ao Ministério Público requerer cautelarmente que os registros de conexão sejam guardados por prazo superior a 1 ano, quais sejam, aqueles exclusivos a informações de data e hora de acesso, duração e IP de origem, o que, como afirmado alhures, não se confunde com o conteúdo telemático armazenado dentro dos sistemas autônomos, tais como históricos de pesquisa, todo o conteúdo de e-mail e *Imessages*, fotos e dados de localização. Entendimento diverso levaria à autorização para que houvesse a busca e apreensão prévia de conteúdos e seu congelamento, para posterior formalização da medida por ordem judicial, em prática vedada por qualquer *standard* que se extraia da ordem constitucional vigente.
> Conclui-se, portanto, que, na hipótese sob exame, o Ministério Público do Estado do Paraná não observou a necessária reserva de jurisdição no que toca à ordem de indisponibilidade do conteúdo telemático por parte da sua legítima titular, contrariando, na forma acima delineada, a Constituição Federal e o Marco Civil da Internet, pois decretou verdadeira medida cautelar ao ordenar, *sponte própria*, o "congelamento" de todo o conteúdo de comunicações telemáticas da paciente. Em suma, retirou do seu legítimo proprietário o direito de dispor do conteúdo dos seus dados para quaisquer fins, sem que houvesse autorização judicial para tanto[106].

Dessa forma, os registros de conexão são tipos específicos de informação que os provedores de internet devem armazenar acerca das atividades dos usuários, sendo o histórico de presença on-line, como data e hora de início e término, duração e endereço IP. Esse registro é essencial por diversas razões, incluindo a proteção e a apuração de ações ilícitas nas redes. Isso possibilita identificar, se necessário, quem estava acessando a internet em um momento específico e quais atividades estavam sendo realizadas, dentro de certos limites. No entanto, é crucial que essas informações sejam protegidas para garantir a confidencialidade e a privacidade dos usuários. Por tal razão, o MCI define normas para a guarda e acesso a tais dados. Assim, a lei somente autoriza ao MP o requerimento de preservação dos registros de

[106] HABEAS CORPUS 222.141 PARANÁ. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/HC222141.pdf. Acesso em: 18 jul. 2024 .

conexão, e não mais do que isso, como ocorreu no caso ora narrado. Para tanto, seria necessária autorização judicial, já que o pedido vai além do disposto no art. 13, § 2º do MCI[107].

Dito por outras palavras, a proteção das informações pessoais contidas em e-mails, mensagens, contatos e registros de localização só pode ser reduzida sob a perspectiva constitucional em situações expressamente previstas por lei e com a devida autorização judicial. Uma interpretação diferente permitiria que autoridades de investigação realizassem buscas e apreensões de conteúdo antes de qualquer decisão judicial, com o objetivo de posteriormente formalizar essa ação por meio de uma ordem judicial, o que constitui uma prática proibida pela constituição atual[108].

Imperioso destacar que, na provisão de conexão, é vedado guardar os registros de acesso a aplicações de internet (art. 14). Dessa forma:

> [...] pela dinâmica dos arts. 13 e 14 o provedor de conexão deve guardar os registros dos *sites* acessados pelos seus usuários (data, hora, endereço eletrônico), mas não pode guardar o teor do que foi acessado, ou seja, as aplicações de internet (conteúdos).
> A vedação do art. 14 quanto aos provedores de conexão não poderem guardar os registros de acesso às aplicações de internet (conteúdos) pelo usuário está relacionada à prática, até então comum, desses provedores de aproveitarem a captação de dados relacionados às preferências dos internautas para realizarem anúncios dirigidos conforme seus gostos pessoais (*marketing* eletrônico)[109].

Os provedores de aplicações de internet devem manter os registros de aplicação sob sigilo e em ambiente controlado e de segurança pelo prazo de seis meses (art. 15), desde que se trate de pessoa jurídica e que exerça a atividade de forma organizada, profissionalmente e com fins econômicos; do contrário, deve haver ordem judicial para determinar a guarda por determinado período (art. 15, § 1º)[110].

---

[107] CAVALCANTE, Márcio André Lopes. São nulas as provas obtidas a partir de dados preservados em contas da internet (com o congelamento e a consequente perda da disponibilidade), mediante requerimento do Ministério Público, sem a prévia autorização judicial de quebra de sigilo e fora das hipóteses legais**. Buscador Dizer o Direito**, Manaus. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/0dd4f2526c7c874d06f19523264f6552. Acesso em: 23 out. 2024.

[108] CAVALCANTE, loc. cit.

[109] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 95.

[110] É importante transcrever outros pontos do dispositivo: § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13. § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo. § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

De todo modo, a lei também estabelece que a opção por não guardar os registros de acesso não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros (art. 17).

Quanto à responsabilidade por danos, o MCI determina expressamente que o provedor de conexão não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros (art. 18); assim, da mesma maneira que uma empresa de telefonia não é responsabilizada pelo uso inadequado de suas linhas para fins criminosos, o provedor de internet não será punido pelo uso impróprio do acesso por parte de seu usuário que resulte em prejuízo a terceiros, como acontece, por exemplo, com o envio de spam (mensagens indesejadas) ou contendo vírus de computador[111].

Contudo, existindo ordem judicial para a retirada de determinado conteúdo, caberá ao provedor retirá-lo da rede e, se não o fizer dentro do prazo assinalado, poderá ser responsabilizado em relação aos danos decorrentes do conteúdo gerado por terceiros (art. 19)[112].

O art. 19 do Marco Civil da Internet assim dispõe:

> Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário[113].

---

[111] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 97.

[112] A jurisprudência do Superior Tribunal de Justiça (REsp 2.129.749-SP), no sentido de que ainda que não seja responsável pela fiscalização prévia do conteúdo publicado, a plataforma somente seria responsabilizada civilmente se, após ordem judicial específica, não tomasse as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente (com a exceção dos casos que envolverem nudez ou atos sexuais privados, cuja retirada independe de ordem judicial). Ademais, estipulou-se a obrigatoriedade de o requerente indicar de forma clara e específica o URL do conteúdo que pretende que seja retirado (REsp nº 1.642.560/SP, relator Ministro Marco Aurélio Bellizze, relatora para acórdão Ministra Nancy Andrighi, Terceira Turma, julgado em 12/9/2017, DJe de 29/11/2017, REsp nº 1.679.465/SP, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 13/3/2018, DJe de 19/3/2018, AgInt no AREsp nº 685.720/SP, relator Ministro Marco Buzzi, Quarta Turma, julgado em 13/10/2020, DJe de 16/10/2020, e REsp nº 2.088.236/PR, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 23/4/2024, DJe de 26/4/2024)"

[113] Também consta no dispositivo que: § 1º A ordem judicial de que trata o **caput** deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material. § 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal. § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais. § 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Importante ressaltar a decisão do C. Superior Tribunal de Justiça, no REsp 2.139.749-SP, de relatoria do Ministro Ricardo Villas Bôas Cueva, julgado em 27/08/2024, que entendeu que o provedor de aplicação de internet pode, ainda que por iniciativa própria e sem ordem judicial, retirar de sua plataforma conteúdos que violem a lei ou seus termos de uso. Isso porque os termos de uso estão, precipuamente, subordinados aos preceitos constitucionais, de modo que a moderação de conteúdo encontra fundamento de ser dentro do ecossistema da internet. Assim constou no julgado:

> RECURSO ESPECIAL. MARCO CIVIL DA INTERNET. PROVEDOR DE APLICAÇÃO, PLATAFORMA DE VÍDEO. PANDEMIA DA COVID-19. TERMOS DE USO. DESINFORMAÇÃO. MODERAÇÃO DE CONTEÚDO. REMOÇÃO. LEGITIMIDADE. NOTIFICAÇÃO PRÉVIA. SHADOWBANNING. NÃO OCORRÊNCIA. LIBERDADE DE EXPRESSÃO. CONDICIONANTES.
> [...] 4. Os termos de uso dos provedores de aplicação, que autorizam a moderação de conteúdo, devem estar subordinados à Constituição, às leis e a toda regulamentação aplicável direta ou indiretamente ao ecossistema da internet, sob pena de responsabilização da plataforma.
> 5. Moderação de conteúdo refere-se à faculdade reconhecida de as plataformas digitais estabelecerem normas para o uso de espaço que disponibilizam a terceiros, que podem incluir a capacidade de remover, suspender ou tornar indispensáveis conteúdos ou contas de usuários que violem essas normas.
> 6. O art. 19 da Lei Federal nº 12.965/2014 (“Marco Civil da Internet”) não impede nem proíbe que o próprio provedor retire de sua plataforma o conteúdo que violar a lei ou os seus termos de uso. Essa retirada pode ser reconhecida como uma atividade lícita de *compliance* interno da empresa, que estará sujeita à responsabilização por eventual retirada indevida que venha a causar prejuízo injustificado ao usuário.
> 7. *Shadowbanning* consiste na moderação de conteúdo por meio do bloqueio ou restrição de um usuário ou de seu conteúdo, de modo que o banimento seja de difícil detecção pelo usuário (assimetria informacional e hipossuficiência técnica). Pode ser realizado tanto por funcionários do aplicativo quanto por algoritmos e, em tese, caracterizar ato ilícito, arbitrariedade ou abuso de poder. Não ocorrência, no presente caso.
> 8. Recurso especial parcialmente conhecido e não provido [...]
> Não se sustenta a interpretação levantada pelo recorrente, de que o provedor poderia tornar o conteúdo indisponível se, e somente se, houvesse ordem judicial específica para tanto.
> A regra do art. 19 do Marco Civil da Internet busca equilibrar, no campo normativo, o comportamento do provedor de aplicações de internet no que se refere à liberdade de expressão, à vedação da censura e à responsabilização da plataforma decorrente de conteúdo gerado por terceiros, bem como a eventual necessidade de remoção de tal conteúdo.
> A análise da legalidade da retirada, por iniciativa própria, de conteúdos que violem os termos de uso, as políticas e as diretrizes da comunidade, questão central deste recurso, por sua vez, também guarda relação de equilíbrio entre a conduta do provedor de aplicações e os valores conformados nesse dispositivo legal [...]
> De maneira geral, os termos de uso e seus correlatos (termos e condições, políticas de privacidade, diretrizes da comunidade, regras de serviço etc.) representam um conjunto de orientações padronizadas e definidas de formas unilateral pelas empresas de internet, que são oferecidas a todo e qualquer usuário dos seus serviços, a fim de regular a relação entre eles.
> Essas cláusulas, reconhecidas por muitos como um autêntico contrato de adesão, impostas aos usuários por esses provedores e obrigam as partes a cumprirem todas as disposições ali estabelecidas [...]

> Embora estabelecidas unilateralmente, o fato é que as disposições dos termos de uso devem estar subordinadas e alinhadas aos parâmetros regulatórios estabelecidos para o ecossistema da internet, assim como suas cláusulas estarão sempre sujeitas ao controle judicial, haja vista a permanente possibilidade de violação de direitos de usuários ou de terceiros, com destaque para a característica das relações no ambiente digital com esses provedores, em que a assimetria técnica, informacional e o poder econômico de empresas responsáveis por grandes plataformas têm o potencial de comprometer a isonomia entre as partes. Dado esse cenário, verifica-se que as plataformas têm todo o incentivo para cumprir não apenas a lei, mas, fundamentalmente, os seus próprios termos de uso (admitindo-se que eles estão em conformidade com o ordenamento jurídico), objetivando evitar, mitigar ou minimizar eventuais contestações judiciais ou mesmo extrajudiciais. Assim, é legítimo que um provedor de aplicação de internet, mesmo sem ordem judicial, retire de sua plataforma determinado conteúdo (texto, mensagem, vídeo, desenho etc.) quando este violar a lei ou seus termos de uso, exercendo uma espécie de autorregulação regulada: autorregulação ao observar suas próprias diretrizes de uso, regulada pelo Poder Judiciário nos casos de excessos e ilegalidades porventura praticados[114].

Dessa forma, vê-se que a retirada é forma lícita de compliance interno da empresa, não havendo qualquer violação à liberdade de expressão ou outros princípios entabulados, principalmente no MCI.

Além disso, a lei conferiu tratamento especial em relação a cenas de nudez ou de atos sexuais, no sentido de que o provedor que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação sem autorização, se, após o recebimento de notificação, deixar de promover, de forma diligente, a indisponibilização do conteúdo (art. 21, caput)[115].

O C. STJ foi além, entendendo que "*para atender ao princípio da proteção integral, é dever do provedor de aplicação de internet proceder à retirada de conteúdo que viola direitos de crianças e adolescentes assim que for comunicado do caráter ofensivo da publicação, independentemente de ordem judicial"* (STJ, 4ª Turma, REsp 1783269-MG, de Relatoria do Ministro Antônio Carlos Ferreira, julgado em 14/12/2021 – Informativo 723).

Mas, como já mencionado, as particularidades de cada caso concreto deverão ser levadas em conta. No julgamento do REsp 1.930.256-SP, de relatoria da Ministra Nancy Andrigui, julgado em 07/12/2021, o STJ, analisando caso versando sobre modelo que realizou ensaio fotográfico de nudez para revista masculina e que passou a encontrar as fotos em blogs hospedados no Google sem autorização, entendeu que não há caráter privado a atrair a aplicação do art. 21 do MCI, sendo que "*nem toda divulgação indevida de material de nudez ou de*

---

[114] BRASIL. Superior Tribunal de Justiça. **REsp nº 2.139.749/SP** (2023/0068660-0), Relator Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 27/08/2024, DJe 30/08/2024.

[115] MCI, art. 21, parágrafo único - A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

conteúdo sexual atrai a regra do art. 21, mas apenas aquele que apresenta, intrinsecamente, uma natureza privada", daí porque o "*ensaio fotográfico de nudez realizado especificamente para sua exploração econômica por revista adulta, voltada para público seleto mediante pagamento pelo acesso no seu website, não pode mesmo ser definida como de caráter privado"* (Informativo 721).

O MCI também trata da possibilidade de requerimento ao juiz para que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet, com o fim de formar conjunto probatório em processo judicial. E, dentro desse panorama, cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, vida privada, honra e imagem do usuário, podendo, inclusive, determinar segredo de justiça (arts. 22 e 23).

Nesse sentido, a já mencionada decisão no RMS nº 61.302/RJ, do C. STJ:

> [...] 7. Os arts. 22 e 23 do Marco Civil da Internet, que tratam especificamente do procedimento de que cuidam os autos, não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Assim, para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros. Não é necessário, portanto, que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação, tampouco que justifique a indispensabilidade da medida, ou seja, que a prova da infração não pode ser realizada por outros meios, o que, aliás, seria até, na espécie – se houvesse tal obrigatoriedade legal – plenamente dedutível da complexidade e da dificuldade de identificação da autoria medida dos crimes investigados.
> 8. Logo, a quebra do sigilo de dados armazenados, de forma autônoma ou associada a outros dados pessoais e informações, não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas, até porque o objetivo precípuo dessa medida, na expressiva maioria dos casos, é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado.

O MCI também prevê diversas diretrizes para a atuação da União, Estados, Distrito Federal e Municípios quanto ao desenvolvimento da internet no Brasil, a saber: (i) estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica; (ii) promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil; (iii) promoção da racionalização e interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos; (iv) promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade; (v) adoção

preferencial de tecnologias, padrões e formatos abertos e livres; (vi) publicidade e disseminação de dados e informações públicas, de forma aberta e estruturada; (vii) otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa; (viii) desenvolvimento de ações e programas de capacitação para uso da internet; (ix) promoção da cultura e da cidadania; e (x) prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos (art. 24).

Ainda, o MCI estabeleceu orientações para as aplicações de internet nos sites dos entes públicos: (i) compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso; (ii) acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais; (iii) compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações; (iv) facilidade de uso dos serviços de governo eletrônico; e (v) fortalecimento da participação social nas políticas públicas (art. 25).

Também expressa o cumprimento do dever constitucional do Estado na prestação da educação em todos os níveis de ensino, incluindo "a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico" (art. 26).

Além disso, existe a possibilidade de controle parental de conteúdo também (art. 29)[116]. Segundo Tarcísio Teixeira:

> [...] o controle parental está relacionado ao poder familiar (ou pátrio poder), que consiste na relação entre pais e filhos do ponto de vista dos deveres e direitos a serem exercidos por aqueles sobre estes, ficando os filhos sujeitos ao poder familiar especialmente no campo da educação e assistência, bem como com o dever de prestar obediência (Código Civil, arts. 1.630 a 1.638). Controle parental no uso da internet são as limitações e restrições estabelecidas pelos detentores do poder familiar, essencialmente via instalação de *softwares*, quanto ao tempo de navegação e ao acesso a certos *sites* e/ou conteúdos disponíveis na internet[117].

[116] MCI, art. 29 - O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei da Lei nº 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente. Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no caput, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

[117] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 104.

Ainda nesse sentido, as iniciativas públicas de fomento à cultura digital e promoção da internet como ferramenta social, com promoção da inclusão digital, busca quanto à redução das desigualdades (sobretudo entre as diferentes regiões do país), além de fomentar a produção e circulação de conteúdo (art. 27), sendo que o Estado deve, "periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País" (art. 28).

Após análise do Marco Civil da Internet (MCI), pode-se concluir que hoje, em uma época marcada por uma sociedade (quase completamente informatizada), em que não apenas as opiniões, mas as tarefas do dia a dia são compartilhadas e realizadas por meio de redes sociais e plataformas on-line, todos os princípios elencados no referido diploma legal desempenham um papel fundamental na preservação do Estado Democrático de Direito.

2.4 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) - LEI 13.709/2018

2.4.1 Considerações iniciais: princípios, dados pessoais, acesso e direitos do titular

Diante de toda a mudança no cenário mundial trazida pela internet, surgiu um problema: a questão acerca da proteção de dados, afinal, com a utilização de informações pessoais por empresas e entidades governamentais, tornou-se imprescindível uma legislação destinada à tutela.

Aliás, o próprio MCI reconhecia a necessidade de lei específica, notadamente no art. 3º, inciso III que, ao expressar que a proteção de dados é princípio legal, faz ressalva ao mencionar que deve ser feito "na forma da lei". Como visto, o MCI possui extensas disposições sobre privacidade, mas não é diploma de proteção de dados.

O debate sobre a importância de uma proteção legal para os dados e a privacidade das pessoas começou na Europa na década de 1970, resultando na Diretiva n. 95/46/CE, que, posteriormente, foi substituída pelo Regulamento n. 2016/679 (*General Data Protection Regulation* - GDPR; em português, Regulamento Geral de Proteção de Dados Pessoais – RGPD), que entrou em vigor em 2018[118], com foco na elaboração de normas e diretrizes a respeito da proteção das pessoas físicas, definindo regras para o tratamento de dados pessoais por pessoas, empresas ou organizações, com objetivo de "contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico

[118] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 107.

e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares"[119].

No Brasil, em 2018, surge a Lei Geral de Proteção de Dados, elencando 65 artigos, tendo como objetivo a proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento (art. 1º) e, desde 1º de agosto de 2021, está totalmente em vigor[120].

Nesse sentido, destaca Thomas Law:

> [...] em termos de proteção de dados, a Lei Geral de Proteção de Dados de 2018 pode ser considerada a primeira lei geral do Brasil, pois se concentra exclusivamente no tema e pode ser aplicada sem distinção a qualquer processamento de dados pessoais (realizado em mídia digital e *off-line*), por qualquer pessoa, em qualquer setor, afora as exceções estabelecidas na própria LGPD. Ou seja, a LGPD é geral no que diz respeito à proteção de dados pessoais no Brasil.
> No entanto, quando comparada ao Marco Civil da Internet – que regula vários outros tópicos -, a Lei Geral de Proteção de Dados pode ser considerada um regulamento especial. Isso ocorre porque não existe uma lei propriamente dita, sempre geral ou sempre especial. A relação de especialidade surge da comparação de duas ou mais leis em uma determinação situação [...] Portanto, mesmo que o Marco Civil também aborde a proteção de dados pessoais, ele regula uma série de outros temas, enquanto a LGPD é específica para o processamento de dados pessoais, abordando-o em detalhe e de maneira abrangente. Em resumo, ao considerar apenas o microssistema de proteção de dados pessoais, a LGPD seria geral em relação às várias leis setoriais que também tratam do assunto, como o Código de Defesa do Consumidor [...][121].

A lei também disciplina os fundamentos (art. 2º), a saber:

> I – o respeito à privacidade;
> II – a autodeterminação informativa;
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
> IV – a inviolabilidade da intimidade, da honra e da imagem;
> V – o desenvolvimento econômico e tecnológico e a inovação;
> VI – a livre iniciativa, a livre concorrência e a defesa do consumidor;
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

---

[119] UNIÃO EUROPEIA. Legislação - **Jornal Oficial da União Europeia**, 4 maio 2016. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN. Acesso em: 10 out. 2024.

[120] "Inicialmente a lei brasileira tinha uma *vacatio legis* (tempo para entrar em vigor uma lei) de 18 meses, mas, com as alterações promovidas pela Lei n. 13.853/2019 (lei que cria a ANPD – Autoridade Nacional de Proteção de Dados), o prazo de início da vigência da LGPD foi ampliado para 2 anos, igualando assim a lei europeia. A LGPD teve sua vigência inicial fatiada, porém, desde o dia 1º de agosto de 2021, está totalmente em vigor" (conforme TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 107-108). Ainda, "A LGPD entraria em vigor em agosto de 2020 – mas foi adiada em decorrência da crise do COVID-19. Em tal contexto, a LGPD passou a ser vigente [...] em 17 de setembro de 2020 – enquanto a possibilidade de aplicação de sanções restou adiada para agosto de 2021 [...] dupla *vacatio legis* que se estabeleceu, e consequente vigência de uma lei temporariamente sem sanções [...]", (MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 118-119).

[121] LAW, Thomas. **A Lei Geral de Proteção de Dados – LGPD.** Uma análise comparada ao novo modelo chinês. São Paulo: D'Plácido, 2021, p. 285-286.

A LGPD é aplicada às operações de tratamento (realizadas tanto por pessoa natural quanto jurídica de direito público ou privado), independentemente do meio, desde que: (i) realizada no território nacional; (ii) tenha por objetivo a oferta ou fornecimento de bens ou serviço ou tratamento de dados de indivíduos localizados no território nacional; e (iii) os dados pessoais tenham sido coletados no território nacional (art. 3º[122]).

No entanto, a LGPD não se aplica (conforme art. 4º), ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos (inciso I), quando realizados para fins exclusivamente jornalístico e artísticos ou acadêmicos (inciso II[123]), realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (inciso III) ou provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD (inciso IV[124]).

Ao tratar dos dados, o art. 5º determina diversos conceitos:

> I – **dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;
> II – **dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;[125]
> III – **dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV – **banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

---

[122] Art. 3º, § 1º. Consideram-se coletados no território nacional de dados pessoais cujo titular nele se encontre no momento da coleta.

[123] Aplicando-se, na hipótese de tratamento de dados pessoais acadêmicos, os artigos 7º e 11 da Lei.

[124] Nesse sentido, também estabelece o art. 4º.

§ 1º. O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

[125] Como ressalta Tarcísio Teixeira, "a íris dos olhos e a impressão digital dos dedos são tidos como dados sensíveis" (TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 110).

> V – **titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;[126]
> VI – **controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII – **operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII – **encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX – **agentes de tratamento:** o controlador e o operador;
> X – **tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI – **anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII – **consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> XIII – **bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> XIV – **eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
> XV – **transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
> XVI – **uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de banco de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para um ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
> XVII – **relatório de impacto à proteção de dados pessoais:** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
> XVIII – **órgão de pesquisa:** órgão ou entidade da administração pública direta ou indireta ou a pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, como sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e
> XIX – **autoridade nacional:** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (grifos nossos).

Como visto, o artigo supracitado trata, em sentido amplo, do que é dado pessoal. Dessa forma, será nome e número de algum documento, por exemplo, ou que possa levar à identificação como a soma de informações relativas às características. Em suma, "dados pessoais diretos quando as informações identifiquem diretamente a pessoa. Já os dados pessoais indiretos quando a pessoa puder ser identificada (identificável) pelas informações"[127].

No que tange à "anonimização" (dados anonimizados), Amanda Martins ressalta que:

---

[126] Imperioso destacar que pessoas jurídicas não são titulares de dados pessoais para efeitos desta lei.
[127] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 108.

> [...] se por um lado, há críticas sobre os limites da anonimização, já que uma pequena quantidade de dados, mesmo que anônimos, pode permitir a identificação do seu titular (danos anonimizados, portanto, porém identificáveis), por outro lado o desenvolvimento da tecnologia de *blockchain* [...] permite que as informações sejam criptografadas e permaneçam seguras em uma cadeia de informação, preservando-se seu sigilo (devido à necessidade de chave) e sua correção (pois os dados são inalteráveis) [...]
> Todas essas informações são passíveis de serem obtidas por meio da *internet*: o acesso a *websites* ou o cadastro em páginas de instituições religiosas, a utilização de redes sociais voltadas para relacionamentos pessoais, informações sobre resultados de exames médicos e uma série incontável de dados sensíveis são fornecidos a todo tempo a empresas responsáveis pelo seu tratamento, muitas vezes desprotegidas quanto ao acesso por particulares, criminosos, agências governamentais ou *hackers*[128].

O art. 12[129] da Lei reforça que "os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido".

Além desses, existem os dados pseudonimizados, sendo "o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (art. 13, § 4º).

Assim, a "anonimização de dados difere da pseudonimização de dados, em que os dados ainda podem ser associados a uma pessoa em razão de um elemento de ligação que fica registrado separadamente"[130].

Em suma, e acerca das diferenciações sobre dados pessoais e dados sensíveis, enquanto aqueles estão relacionados à privacidade do titular, estes dizem respeito à intimidade[131].

A LGPD também afirma que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios (art. 6º):

> I - **finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - **adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

---

[128] MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 123-124.
[129] Art. 12. § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.
§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.
[130] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 109.
[131] Ibid., p. 110.

> III - **necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - **livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - **qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - **transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - **segurança:** utilização de medidas 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;
> VIII - **prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - **não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e
> X - **responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (grifos nossos).

Acerca dos princípios, destaca Amanda Martins:

> No que tange ao princípio da **finalidade** [...] implica a possibilidade de utilização dos dados para além daquele fim que foi expressamente acordado entre as partes quando cedidos.
> O princípio da **adequação** [...] não basta que o uso das informações ou dados seja para o fim para o qual foi informado – é necessário que tal uso seja adequado, compatível com aquilo que foi informado e expressamente acordado no momento da cessão dos dados.
> [...] princípio da **necessidade** [...] Os princípios da proporcionalidade e da adequação são frequentemente invocados em matéria de responsabilidade civil, de modo que é imprescindível que o uso dos dados não se dê de forma abusiva, ou além do necessário ou daquilo que foi pactuado ou expressamente informado.
> O quarto princípio constante na Lei é o princípio do **livre acesso** aos dados [...] Após a cessão dos dados pessoais, o indivíduo deve conhecer os responsáveis pelo seu armazenamento, bem como o prazo em que eles serão tratados. Ainda, é importante que lhe seja possível ter acesso aos dados que foram cedidos, de forma "facilitada e gratuita".
> A **qualidade dos dados**, por sua vez, refere-se à clareza, atualidade, precisão e veracidade das informações, em conformidade com a finalidade do tratamento. Sob este aspecto, destaca-se o direito do titular dos dados solicitar a retificação ou correção de dados, conforme necessário. Para isso, é imprescindível que tenha acesso aos dados coletados.
> O princípio da **transparência** está relacionado ao princípio do livre acesso aos dados [...] trata-se do direito de acesso aos dados que foram cedidos, bem como as informações sobre os agentes ou empresas que possuem acesso a eles, e que podem utilizá-los.
> O sétimo princípio – princípio da **segurança** [...] visa obstar a utilização inadequada de dados pessoais quando tal tratamento de dados se der em desacordo com os princípios anteriormente elencados.
> Já o princípio da **prevenção** necessita que as empresas adotem medidas prévias a fim de evitar a ocorrência de danos decorrentes do tratamento de dados. Desse modo, a privacidade desde a concepção mostra-se indispensável, bem como a adoção de medidas de segurança, o que evita o roubo ou o vazamento de base de dados.

> O penúltimo princípio trata sobre a **não discriminação** [...] Trata-se de medida essencial para garantir o acesso igualitário aos dados e à informação, em conformidade com os princípios constitucionais, bem como para coibir práticas abusivas e ilícitas, as quais podem ser facilitadas pela utilização de meios de comunicação, como a *internet*.
> Por fim, o último princípio elencado é o da **responsabilização e prestação de contas** [...] trata-se de disposição relevante para garantir a segurança do tratamento conferido aos dados pessoais no ambiente *on-line*, especialmente quando tal tratamento se der por agências governamentais[132].

A LGPD também estabelece que o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (i) mediante o fornecimento de consentimento pelo titular[133]; (ii) para o cumprimento de obrigação legal ou regulatória pelo controlador; (iii) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; (iv) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (v) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; (vi) para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); (vii) para a proteção da vida ou da incolumidade física do titular ou de terceiro; (viii) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (ix) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou (x) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (art. 7º).

Como não poderia deixar de ser, o tratamento de dados deve considerar a finalidade, a boa-fé e o interesse público que justificaram a disponibilização (art. 7º, § 3º)[134].

---

[132] MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 127-129.

[133] Neste caso, o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º).

[134] LGPD, art. 7º, § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei. § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei. § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular. § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

Acerca do consentimento, previsto no art. 8º[135]:

> [...] deverá ser fornecido por escrito ou via outro meio que demonstre a manifestação de vontade do titular, por exemplo, utilizando-se de ferramentas digitais/eletrônicas como o e-mail, o WhatsApp etc.
> Sendo o consentimento do titular fornecido por escrito, ele deverá estar asseverado em cláusula destacada das demais (cláusulas contratuais). Isto é, o titular deve ser informado ostensivamente sobre a necessidade de seu consentimento para aquele negócio que se tem projetado. Compreendemos que essa cláusula destacada deve ser observada em contratos físicos e/ou eletrônicos, estando aqui incluídos os Termos de Uso e Políticas de Privacidade empregados por plataformas digitais (sites, blogs etc.).
> O ônus da prova de que o consentimento foi obtido nos termos da Lei de Proteção de Dados é do controlador (pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais), conforme os termos do § 2º do art. 8º, c/c o inc. VI do art. 5º.
> Além disso, o § 3º do art. 8º é claro ao expressar a proibição de tratamento de dados pessoais mediante vício de consentimento. Logo, o consentimento obtido com vício não produzirá efeito para o titular.
> No mais, o consentimento deve estar relacionado a objetivos certos e específicos (por exemplo, para qualificar o consumidor no contrato a ser firmado com o fornecedor) e não a autorizações genéricas, sob pena de o consentimento ser nulo.
> A lei dispõe sobre a possibilidade de o titular do dado revogar seu consentimento. Isso pode ser feito a qualquer tempo por sua manifestação expressa via procedimento facilitado e não oneroso (gratuito). Mesmo com a revogação, permanecerão ratificados os tratamentos realizados sob o consentimento outrora manifestado, salvo se houver requerimento de eliminação (§ 5º do art. 8º, c/c o inc. VI do caput do art. 18).
> Se houver alguma alteração em uma das hipóteses a seguir descritas, é obrigação do controlador informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração (§ 6º do art. 8º, c/c os incs. I, II, III e V do art. 9º). São as hipóteses de alteração quanto:
> A – à finalidade específica do tratamento;
> B – à forma e duração do tratamento, observados os segredos comercial e industrial;
> C – à identificação do controlador;
> D – às informações acerca do uso compartilhado de dados pelo controlador e a finalidade.
> Vale reforçar que, se o consentimento do titular dos fatos foi exigido em qualquer das hipóteses acima, ele poderá revogá-lo se discordar da alteração[136].

[135] Art. 8º, § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.
[136] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 116.

O artigo 10 trata do legítimo interesse acerca do tratamento de dados pelo controlador, consideradas as seguintes situações concretas, que incluem, mas não se limitam a: (i) apoio e promoção de atividades do controlador; e (ii) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais (em conformidade com os preceitos da LGPD).

O § 1º do artigo 10 estabelece que somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, quando o tratamento for baseado no legítimo interesse do controlador. Ainda, o § 2º determina que o controlador deverá adotar medidas para garantir a transparência do tratamento de dados. Por fim, ao § 3º estabelece que a autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais (RIPD), quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Acerca do tratamento de dados pessoais sensíveis, poderá ocorrer nas seguintes hipóteses: (i) quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; ou (ii) sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (art. 11).

A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com o objetivo de obter vantagem econômica pode ser objeto de vedação ou de regulamentação por parte da autoridade nacional (art. 11, § 3º). Contudo, é vedada a comunicação ou uso compartilhado de dados referente à saúde com o objetivo de obter vantagem econômicas, exceto nas hipóteses relativas à prestação de serviços de saúde, assistência farmacêutica e de saúde, desde que não seja para seleção de riscos na contratação ou exclusão de beneficiários (art. 11,

§§ 4º e 5º), o que se aplica igualmente à situação em que a operadora pretende estabelecer um período de carência para doenças consideradas preexistentes, das quais obteve conhecimento por meio de acesso indevido aos dados[137]. Também reservou tratamento específico para os dados pessoais de crianças e adolescentes, sempre atentando ao melhor interesse (art. 14)[138].

O tratamento de dados tem início, meio e fim, sendo que o término ocorrerá nas seguintes hipóteses: (i) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) fim do período de tratamento; (iii) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou (iv) determinação da autoridade nacional, quando houver violação ao disposto nesta Lei (art. 15).

Ainda, os dados serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: (i) cumprimento de obrigação legal ou regulatória pelo controlador; (ii) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados disposto nesta Lei; ou (iv) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (art. 16).

Noutro giro, também elenca os direitos do titular, sendo que toda pessoa natural tem assegurada a titularidade de seus dados pessoais, "garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade" (art. 17). Ademais, tem direito a obter do controlador, em relação aos dados do titular, a qualquer momento e mediante requisição: (i) confirmação da existência de tratamento; (ii) acesso aos dados; (iii) correção de dados

---

[137] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 122.

[138] LGPD, art. 14. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei. § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo. § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis. § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; (v) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (vi) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; (vii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e (ix) revogação do consentimento, nos termos do § 5º do art. 8º desta Lei (art. 18[139]).

Os direitos previstos serão exercidos mediante requerimento expresso do titular ou representante constituído legalmente (art. 18, § 3º), que será atendido sem custos para o titular (art. 18, § 5º).

O titular também tem direito, na esfera administrativa, de peticionar contra o controlador em relação aos seus dados, junto à autoridade nacional, também podendo exercer tal direito perante os organismos de defesa do consumidor (art. 18, § 1º e 8º).

Também terá direito a oposição ao tratamento, com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD (art. 18, § 2º).

Se o controlador não puder atender imediatamente à solicitação, enviar resposta: (i) comunicando que não é agente de tratamento dos dados e indicando, quando possível, o agente; ou (ii) indicando as razões de fato ou de direito que impedem a adoção imediata da providência (art. 18, § 4º).

E, caso tenha ocorrido o compartilhamento de dados, deverá o responsável informar imediatamente aos agentes de tratamento a eliminação, correção, anonimização ou bloqueio, salvo se a comunicação seja – comprovadamente – impossível ou implique esforço desproporcional (art. 18, § 6º).

A resposta acerca da existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: (i) em formato simplificado, imediatamente; ou (ii) por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular (art. 19).

[139] Art. 18, § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

A ANPD também poderá dispor de forma diferenciada acerca dos prazos previstos (art. 19, § 4º). A critério do titular, as informações poderão ser fornecidas: (i) por meio eletrônico, seguro e idôneo para esse fim; ou (ii) sob forma impressa (art. 19, § 2º). Ainda:

> Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento (art. 19, § 3º).

A LGPD determina que os dados pessoais serão armazenados em formato que favoreça o exercício do direito de dados (art. 19, § 1º). Contudo, essa regra pode comprometer a proteção das informações, pois um armazenamento que facilite o acesso ou a realização do direito de acesso pelo proprietário pode ser mais vulnerável a incidentes de segurança, como invasões e alteração de dados, por exemplo[140].

Além disso, o titular de dados pessoais tem o direito de revisão de decisões tomadas unicamente com base no tratamento automatizado dos dados, caso afetem seus interesses. Aqui, incluídas as decisões destinadas a definir perfil pessoal, profissional, de crédito e de consumo, além dos aspectos de sua personalidade (art. 20).

Nesse sentido, a "automatização em tratamento de dados é baseada em softwares e/ou inteligência artificial que facilitam a formação de perfil dos usuários, mas que podem equivocar-se e assim afrontar os interesses dos titulares"[141], sendo certo que o controlador deverá fornecer, sempre que solicitado, as informações de forma clara e adequada a respeito dos critérios utilizados para a decisão automatizada – evidente que também observados os segredos comercial e industrial (art. 20, § 1º). Mas, uma vez alegado segredo comercial e industrial e, não havendo o oferecimento das informações com base em tal alegação, a ANPD poderá realizar auditoria para verificação de aspectos discriminatórios (art. 20, § 2º).

No mais, os dados pessoais que se referem ao exercício regular de direitos (por exemplo, a lavratura de um boletim de ocorrência[142]), não poderão ser utilizados em seu prejuízo (art. 21).

Por fim, o art. 22 estabelece que a defesa dos interesses poderá ser exercida em juízo, de maneira individual ou coletiva (art. 22), mas na forma da legislação pertinente, ou seja, CPC, CDC e até mesmo a Lei da Ação Civil Pública.

---

[140] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 127.
[141] TEIXEIRA, loc. cit.
[142] TEIXEIRA, loc. cit.

A partir do que já foi apresentado, é certo que a promulgação da LGPD foi inovadora, "celebrado não apenas pelo mercado jurídico, mas também por empresas dos mais diversos setores, por acadêmicos e ativistas da internet. Certamente tem muito mais prós do que contras"[143].

2.4.2 Tratamento de dados pessoais pelo Poder Público

A LGPD também disciplina o tratamento de dados pessoais pelo Poder Público, dispondo que o uso compartilhado de dados pessoais deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitados os princípios de proteção de dados pessoais (artigo 26).

Existem três figuras importantes quanto à proteção, quais sejam, controlador, operador e o encarregado de dados (em inglês *Data Protection Officer* – DPO).

Nesse sentido, o controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", o operador é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador", ao passo que o encarregado é pessoa "indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD (art. 5º, incisos VI, VII e VIII, respectivamente).

O controlador e operador devem manter registradas as atividades de tratamento dos dados pessoais, principalmente quando fundamentadas no interesse legítimo (art. 37).

Em relação ao controlador, a ANPD poderá solicitar a criação de relatório sobre os impactos na proteção de dados pessoais, incluindo dados sensíveis, relacionados às suas atividades de tratamento de dados, conforme as diretrizes estabelecidas, respeitando os segredos comerciais e industriais (art. 38).

O RIPD deverá conter, no mínimo, a descrição dos dados coletados, bem como a metodologia utilizada para coleta e para garantia da segurança das informações, bem como a análise do controlador em relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (art. 38, parágrafo único).

---

[143] LAW, Thomas. **A Lei Geral de Proteção de Dados – LGPD.** Uma análise comparada ao novo modelo chinês. São Paulo: D'Plácido, 2021, p. 303.

O operador deverá conduzir o tratamento de acordo com as orientações fornecidas pelo controlador, que irá avaliar a conformidade com suas próprias diretrizes e com as normas pertinentes (art. 39).

Dessa forma:

> Veja-se que o controlador, independentemente de estar em conformidade com as normas sobre a proteção de dados, também deverá se preocupar com todas as pessoas que poderão tratar dados em seu nome. Revela-se aqui a importância de o controlador atentar para todas as pessoas que contratar para lidar com tratamento de dados, inclusive se precavendo em contratos e, principalmente, em medidas aplicáveis à proteção de dados. Utiliza-se, nesse caso, o que se chama de *data processing agreement*; em português, acordo de processamento de dados.
> É possível assemelhar a responsabilização do controlador pelos atos de seus operadores à responsabilidade solidária – atribuída aos fornecedores de serviço pelos atos de seus prepostos e representantes autônomos -, prevista no art. 34 do Código de Defesa do Consumidor. Isso para o âmbito das relações de consumo.
> Já nas áreas civil e empresarial, se o preposto agir com culpa, responderá pessoalmente perante o preponente (empresário); se agir com dolo, responderá perante terceiros solidariamente com o preponente. E mais, os preponentes são responsáveis pelos atos de quaisquer prepostos quando praticados dentro do estabelecimento e relativos à atividade da empresa, mesmo que não autorizados por escrito. Se os atos do preposto forem realizados fora do estabelecimento, o preponente estará obrigado nos limites dos poderes conferidos por escrito. Tudo isso conforme os arts. 1.177 e 1.178 do Código Civil[144].

Em relação ao encarregado de dados, o controlador deverá indicá-lo (art. 41), sendo que sua identidade e informações de contato devem ser publicamente divulgadas (art. 41, § 1º). Pode ser pessoa natural, sendo geralmente colaborador interno da empresa, ou também pessoa jurídica (empresa prestadora de serviços)[145].

No GDPR existe a figura do *Data Protection Officer*, que é o oficial de proteção de dados, similar ao encarregado previsto na legislação brasileira.

Quanto à indicação do encarregado:

> Nos termos do art. 41, caput [...] é a pessoa indicada pelo controlador; entretanto, de acordo com o art. 5º, inc. VIII, o encarregado é indicado pelo controlador e pelo operador. Trata-se, portanto, de um equívoco do legislador. No fundo na redação original do art. 5º, inc. VII, a indicação era apenas do controlador, sendo a alteração promovida pela Lei n. 13.853/2019.
> Tendo em vista o que já foi até aqui retratado, nos parece que a competência para escolher o encarregado de dados seja do controlador, até porque o operador é um subordinado a este, independentemente de ser uma empresa que lhe presta serviços. Logo, o operador – por certo – aceitaria e concordaria com a indicação do controlador, o que seria, portanto, mera formalidade. Mas, diante dessa contradição legal, por excesso de cautela, poderá aquele a quem competir implantar as ferramentas jurídicas dentro da instituição aconselhar que a indicação do encarregado seja feita por ambos, controlador e operador.

---

[144] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 129.
[145] Ibid., p. 130.

> Embora a Seção II (Do Encarregado pelo Tratamento de Dados Pessoais) pertença ao Capítulo IV (Dos Agentes de Tratamento de Dados Pessoais), não se pode afirmar categoricamente que o encarregado seja um dos agentes. Isso porque, nos termos do art. 5º, inc. IX, agentes de tratamento são apenas o controlador e o operador. Trata-se de outra contradição da lei[146].

As atividades do encarregado consistem em: (i) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; (ii) receber comunicações da autoridade nacional e adotar providências; (iii) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e (iv) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (art. 41, § 2º). Neste ponto, ressalta Tarcísio Teixeira:

> Nas duas hipóteses [...] (previstas pelo § 2º do art. 41), em que se lê que cabe ao encarregado "adotar providências", isso deve ser compatibilizado com o fato de que o encarregado é nomeado pelo controlador (e operador); logo, não poderá ultrapassar as decisões sobre tratamento de dados tomadas pelo controlador. Entretanto, esse "adotar providências" pode estar associado a novas atribuições do encarregado a serem fixadas pela ANPD, o que de toda sorte pode afrontar as decisões do controlador, gerando algum conflito entre eles e, por consequência, até o rompimento do contrato entre ambos.
> O ideal é que o encarregado atue com a maior imparcialidade possível, como um "oficial de *compliance"*. Não deve se comportar como mero cumpridor de ordens ou um subordinado do controlador, embora remunerado por este. Mas também não pode afrontar determinações do controlador que estejam amparadas por lei[147].

A ANPD poderá estabelecer normas complementares acerca da definição e atribuições do encarregado, até mesmo hipóteses de dispensa da necessidade de sua indicação, a depender da natureza e o porte da entidade ou o volume de operações de tratamento de dados (art. 41, § 3º).

Acerca da responsabilidade por danos, controlador e operador podem ser responsabilizados, solidariamente sendo que o operador responde pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as orientações – lícitas – do controlador, ao passo que os controladores, em razão dos danos ao titular dos dados (art. 42, caput e § 1º), sendo assegurado o direito de regresso contra os demais responsáveis, na medida da participação no evento danoso (art. 42, § 4º). A ressalva acerca da responsabilidade, para ambos, ocorrerá quando provarem: (i) que não realizaram o tratamento de dados pessoais que lhes é atribuído; (ii) que, embora tenham realizado o tratamento de dados

[146] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 130.
[147] Ibid., p. 131.

pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou (iii) que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (art. 43).

Sobre o tema:

> [...] vale destacar a relevância de uma elaboração minuciosa e criteriosa do contrato firmado entre controlador e operador, visto que será através dele que se poderá apurar quais as instruções dadas pelo controlador e eventual direito de regresso entre ambas as partes, a depender do que estava previsto contratualmente. Vale destacar que empresas precisarão revisar os contratos que já possuem nos seus mais diversos setores/prestadores (Recursos Humanos, *Marketing* etc.) para incluir cláusulas mínimas para compartilhamento de dados entre controlador e operador de forma a regular essa relação. Nesse sentido, a boa elaboração de um contrato contendo as instruções fornecidas pelo controlador ao operador não exime a responsabilidade deste último de verificar se o que lhe está sendo instruído obedecer às normas sobre a matéria (art. 93 da LGPD), não podendo se escusar do cumprimento da lei alegando o cumprimento de ordens ou de cláusulas contratuais. Aqui o "temor reverencial" em razão da hierarquia/subordinação não é excludente de responsabilidade[148].

Além disso:

> [...] se houver culpa "concorrente" da vítima ou de terceiro, ainda assim o condutor ou operador será responsável pelo dano. Neste caso, havendo culpa concorrente da vítima, é aplicável a regra do art. 945 do Código Civil ao estabelecer que a indenização deve ser fixada considerando a gravidade da culpa da vítima em confronto com a do autor do dano. Ou seja, a culpa concorrente não afasta a responsabilidade do controlador ou do operador; apenas pode atenuar o valor da indenização.
> A culpa "exclusiva" da vítima pode dar-se por ação ou por omissão, ou seja, o seu ato é a única causa do dano; ou quando ele tem acesso a meios para afastar seu próprio prejuízo e não o faz, mesmo que por simples descuido omissivo.
> No âmbito da proteção de dados, pode-se citar a culpa exclusiva da vítima quando, por exemplo, o titular dos dados pessoais os divulga publicamente em plataformas digitais; ou armazena seus dados de forma insegura em um *pen-drive*, o que é esquecido negligentemente em local público.
> No que se refere à hipótese de exclusão da responsabilidade por culpa "exclusiva de terceiro", para a sua aplicação esse terceiro não pode ser alguém que mantenha qualquer tipo de relação com o fornecedor (como comerciantes-intermediários, agentes, funcionários, prepostos em geral etc.). Em sede de tratamento de dados, terceiro é uma pessoa que não se identifique com o controlador ou o operador (que não deixa de ser um fornecedor), nem com o titular dos dados (que não deixa de ser um consumidor).
> Por isso, o terceiro deve ser uma pessoa que não mantenha vínculo com o fornecedor [controlador ou operador], isto é, completamente estranho à cadeia de consumo [ou de tratamento de dados]. Por hipótese, o comerciante que distribui os produtos não pode ser tido como terceiro. O mesmo vale para prepostos, empregados e representantes, porque os riscos da atividade econômica são do fornecedor. É por essa assunção de riscos que o CDC, art. 34, estabelece que o fornecedor é solidariamente responsável pelos atos de seus prepostos ou representantes.
> Ressalte-se que, quando se pensa na excludente da culpa exclusiva de terceiros, em tratamento ilícito de dados, não é possível alegar a hipótese de corrompimento de sistema (invasão de *hackers*, por exemplo) se ficar comprovado que as medidas de segurança adotadas pelo agente de tratamento não seguiram os padrões estabelecidos

[148] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 132.

> no art. 44 da LGPD, cujo dispositivo trata dos defeitos no tratamento de dados pessoais[149].

Portanto, a LGPD deve ser ajustada de forma a se compatibilizar com todo o ordenamento jurídico, vez que o fato princípio, caso fortuito e força maior também são excludentes de responsabilidade nas relações jurídicas que se enquadram na LGPD e no CDC (que é fonte subsidiária)[150].

A Lei expressamente determina, quanto à segurança e sigilo de dados, que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de perda, destruição, alteração comunicação ou qualquer outra forma de tratamento que seja ilícito ou inadequado (art. 46, caput). E não apenas os agentes, mas qualquer pessoa que intervenha em uma das fases de tratamento deve garantir a segurança necessária (art. 47).

No que tange à responsabilidade, importante destacar que o C. Superior Tribunal de Justiça, no AREsp 2.130.619-SP, julgado em 7/3/2023, em voto de relatoria do Min. Francisco Falcão, entendeu que o vazamento de dados pessoais não gera dano moral presumido, salvo, evidentemente, se forem dados sensíveis[151].

Nesse prisma, vê-se a necessidade de adaptação das empresas aos termos da LGPD, com cultura de compliance e segurança da informação, notadamente considerando o volume de dados tratados diariamente e com crescimento exponencial. Nesse sentido, as medidas devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (art. 42, § 2º). Além disso, todos os sistemas devem ser estruturados visando atender aos requisitos de segurança, além dos padrões de boas práticas e de governança e aos princípios gerais (art. 49).

E, diante de todo esse panorama, especialmente acerca da responsabilização, o controlador deve comunicar à ANPD e ao titular, em prazo razoável, a ocorrência de qualquer incidente de segurança que possa acarretar risco ou dano relevante (art. 48, caput e § 1º[152]).

---

[149] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 134-135.
[150] Ibid., p. 139.
[151] DIZER O DIREITO. O vazamento de dados pessoais não gera dano moral presumido. **Dizer o Direito,** 31 mar. 2023. Disponível em: https://www.dizerodireito.com.br/2023/03/o-vazamento-de-dados-pessoais-nao-gera.html. Acesso em: 24 out. 2024.
[152] Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
I - a descrição da natureza dos dados pessoais afetados;
II - as informações sobre os titulares envolvidos;
III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV - os riscos relacionados ao incidente;

Portanto, um dos pontos importantes – e de discussão – diz respeito à adaptação e adequação das empresas que realizam tratamento de dados.

Como se viu, o art. 5º, inc. I estabelece que se considera dado pessoal a "informação relacionada à pessoa natural identificada ou identificável". Dito por outras palavras, pode ser fornecido após o preenchimento de formulário ou até mesmo informações divulgadas por meio de redes sociais, dados em que o "aceite" é conferido pelo próprio usuário. Assim, não existe nenhum anonimato nem sequer na mera navegação pela internet[153].

2.4.3 Boas práticas e governança

A LGPD, conforme artigo 50, caput, impulsiona a adoção de regras de boas práticas e de governança, estabelecendo condições de organização, regime de funcionamento e procedimentos, normas de segurança, padrões técnicos e obrigações específicas, além de ações educativas e mecanismos internos de supervisão e mitigação de riscos[154].

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
I - ampla divulgação do fato em meios de comunicação; e
II - medidas para reverter ou mitigar os efeitos do incidente.
§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

[153] MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 120-121.

[154] Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
I - implementar programa de governança em privacidade que, no mínimo:
a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

Conforme o Instituto Brasileiro de Governança Corporativa (IBGC), governança é:

> [...] um sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em geral. Esse sistema baliza a atuação dos agentes de governança e demais indivíduos de uma organização na busca pelo equilíbrio entre os interesses de todas as partes, contribuindo positivamente para a sociedade e para o meio ambiente[155].

De outro lado, boas práticas revelam o sentido de serem adotadas as melhores técnicas (como canais para denúncias e promoção de iniciativas educativas, por exemplo) e, nesse sentido, programas de compliance são imprescindíveis, pois tratam de procedimentos e regras internas da empresa, a serem observadas como verdadeiras normas, visando a prevenção e o controle de riscos na administração.

Segundo Candeloro, Rizzo e Pinho, compliance é:

> [...] um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados ´riscos de compliance´, a que se sujeitam as instituições no curso de suas atividades[156].
> Isso porque em dado momento, várias nações e seus líderes optaram por combater as ações ilícitas – tanto nas esferas públicas quanto nas privadas – levando à implementação de medidas punitivas e limitadoras para indivíduos e países envolvidos em casos de fraudes, corrupção e lavagem de dinheiro, entre outras práticas, o que culminou inclusive na criação de acordos internacionais[157].

Para tanto, a lei esclarece que a ANPD deve, inclusive, estimular a adoção de padrões técnicos (art. 51).

---

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) conte com planos de resposta a incidentes e remediação; e
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.
§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

[155] IBGC. **Código das melhores práticas de governança corporativa**. 6. ed., 2023, p. 17. Disponível em https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/24640/2023_C%c3%b3digo%20das%20Melhores%20Pr%c3%a1ticas%20de%20Governan%c3%a7a%20Corporativa_6a%20Edi%c3%a7%c3%a3o.pdf. Acesso em: 22 out. 2024.

[156] CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins de; PINHO, Vinícius. ***Compliance*** **60º:** Riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012, p. 30,

[157] SILVA, Lilian Reis da. Benefícios do compliance e da gestão de riscos. **Núcleo do Conhecimento,** 13 dez. 2021. Disponível em https://www.nucleodoconhecimento.com.br/administracao/beneficios-do-compliance. Acesso em: 23 out. 2024.

Tudo isso deve ser considerado também para o campo cibernético (cibersegurança), pois problemas nesse sentido podem reverberar para o mercado de trabalho como um todo, além de ter relevância para as investigações e ações penais. Nesse sentido, vale ressaltar que a empresa KPMG, no Conselho de Administração em que estabeleceu prioridades para a agenda de 2024, ressaltou, em análise incluindo os avanços tecnológicos:

> Em 2023, vimos avanços no desenvolvimento e uso da IA Generativa e a sua capacidade de criar conteúdo novo e original na forma de textos, imagens e vídeos. A IA Generativa vem se tornando, cada vez mais, um tópico relevante de discussão na maior parte dos conselhos de administração, à medida em que se busca entender as oportunidades e os riscos apresentados pela tecnologia – um desafio, visto o ritmo acelerado da evolução tecnológica.
> Os potenciais benefícios dessas novas tecnologias variam de acordo com o setor de atuação da empresa, mas podem incluir a automatização dos processos operacionais, tais como serviço ao cliente, criação de conteúdo, elaboração de produtos, desenvolvimento de planos de *marketing*, aprimoramento dos serviços de saúde e criação de novos medicamentos. Já os riscos significativos incluem resultados imprecisos, violações à privacidade de dados e à segurança cibernética, riscos à propriedade intelectual (compreendendo a divulgação não intencional de informações confidenciais ou de propriedade da empresa e o acesso não intencional à propriedade intelectual de terceiros), além dos riscos de *compliance* que existem e que irão surgir, à medida que obrigações legais vão sendo estabelecidas para regular a IA Generativa[158].

Portanto, a implementação de um sistema de governança da privacidade e proteção de dados, juntamente com a observância de práticas recomendadas, auxilia na melhoria das atividades das empresas, além de salvaguardar a imagem (especialmente quando as reclamações também são realizadas por meio da internet, com uma velocidade muito maior do que vista há anos, por exemplo) e continuidade das atividades. É necessário adotar uma nova mentalidade voltada para a proteção de dados, nos termos da LGPD.

2.4.4 Autoridade Nacional de Proteção de Dados (ANPD)

A ANPD[159] é autarquia de natureza especial, que possui autonomia técnica e decisória, com patrimônio próprio, além de sede e foro no Distrito Federal (art. 55-A).

---

[158] KMPG. Conselho de Administração: Prioridades para a agenda de 2024. **KMPG.** Disponível em: https://assets.kpmg.com/content/dam/kpmg/br/pdf/2024/03/Conselho-de-Administracao-Prioridades-para-a-agenda-de-2024.pdf. Acesso em: 20 out. 2024.

[159] Acerca de seu surgimento, "após muito debate, foi criada como uma autoridade de natureza jurídica transitória, ou seja, em um primeiro momento ela foi concebida como um órgão da administração pública federal, vinculado à Presidência da República (art. 55-A, redação original). Sua criação se deu, especificamente, a partir da edição da Lei n. 18.853/2019, a qual promoveu substanciais alterações e inclusões de vários dispositivos na Lei Geral de Proteção de Dados Pessoais. Além disso, o Decreto n. 10.474/2020 aprovou o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforme cargos em comissão e funções de confiança. Em até 2 anos da data de entrada em vigor da LGPD a autoridade

É composta por diversos entes, assemelhando-se a outros órgãos administrativos (art. 55-C[160]), sendo que o Conselho Diretor é composto por cinco diretores, incluindo o Diretor-Presidente (art. 55-D[161]). É órgão essencial para todo o processo de tratamento de dados – desde a coleta até o descarte – possuindo papel fiscalizador e regulamentador.

Sua estrutura regimental será realizada por ato do Presidente da República, sendo que o Conselho Diretor disporá sobre o regimento interno (art. 55-G, caput e § 1º).

As competências da ANPD são as seguintes: (i) zelar pela proteção dos dados pessoais, nos termos da legislação; (ii) zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (iii) elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (iv) fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (v) apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (vi) promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (vii) promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (viii) estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (ix) promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (x) dispor sobre as

---

poderia ser transformada em entidade da administração pública federal, submetida a um regime autárquico especial e vinculada à Presidência da República. Foi promulgada a Lei n. 14.460, de 25 de outubro de 2022, a qual altera a LGPD (sobretudo o art. 55-A), em especial para transformar a ANPD (Autoridade Nacional de Proteção de Dados) em autarquia de natureza especial e transforma cargos em comissão" (TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 141).

[160] Art. 55-C. A ANPD é composta de: I - Conselho Diretor, órgão máximo de direção; II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; III - Corregedoria; IV - Ouvidoria; V-A - Procuradoria; e VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.

[161] Art. 55-D. § 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. § 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. § 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. § 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. § 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor.

formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (xi) solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (xii) elaborar relatórios de gestão anuais acerca de suas atividades; (xiii) editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (xiv) ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (xv) arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; (xvi) realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (xvii) celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; (xviii) editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (xix) garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); (xx) deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (xxi) comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (xxii) comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; (xxiii) articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (xxiv) implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei (art. 55-J).

Além disso, é possível a aplicação de sanções de cunho administrativo, como advertência, multa e até mesmo bloqueio dos dados pessoais (art. 52[162]).

A expectativa em relação à autoridade é que sua atuação seja distinta de outras entidades semelhantes. Espera-se que ela seja contemporânea e proativa, não se limitando apenas à imposição de penalidades, mas também se engajando de maneira prática, especialmente com os responsáveis pelo tratamento de dados, visando uma transformação real na cultura de proteção de dados[163].

Em várias partes da legislação, o papel da ANPD está relacionado à proteção do segredo comercial e da confidencialidade das informações. Isso ocorre porque, em diversas situações, a

[162] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica.
§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.
§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.
§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995.
§ 6º As sanções previstas nos incisos X, XI e XII do **caput** deste artigo serão aplicadas:
I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do **caput** deste artigo para o mesmo caso concreto; e
II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos.
§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo.

[163] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 142.

implementação dos direitos dos titulares de dados pode conflitar com a salvaguarda do segredo empresarial e da privacidade das informações. Assim, estabelece um meio de comunicação direto entre a sociedade, os responsáveis pelo tratamento de dados e outras entidades, visando investigar possíveis irregularidades no manuseio de informações. Além disso, a ANPD atuará como intermediária na comunicação com organismos internacionais para a promoção de iniciativas de cooperação voltadas para a proteção de dados; desempenhará, portanto, um papel crucial na adaptação da lei para as empresas, considerando seu tamanho e particularidades, ao elaborar normas, procedimentos e regulamentos que sejam simplificados e variados de acordo com cada tipo de empresa[164].

2.4.5 Transferência Internacional de Dados

A LGPD dedica um capítulo inteiro para a questão da transferência internacional de dados (Capítulo V).

Nesse sentido, disciplina expressamente que é permitida nos seguinte casos: (i) para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; (ii) quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; (iii) quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos do direito internacional; (iv) quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; (v) quando a autoridade nacional autorizar a transferência; (vi) quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; (vii) quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público; (viii) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação; ou (ix) quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º (art. 33).

[164] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 146.

O nível de proteção de dados do país estrangeiro será avaliado pela ANPD que levará em consideração diversos pontos, como as normas gerais e setoriais da legislação em vigor no país de destino e também a natureza dos dados (art. 34[165]).

Nesse aspecto, é fundamental também compreender o Direito Material pertinente ao tema de acordo com cada sistema jurídico, uma vez que a natureza transnacional da transferência e a gestão de dados conferem uma dimensão internacional às disputas resultantes, e a legislação vigente pode ser mais ou menos benéfica para as partes envolvidas. Nesse aspecto, fica evidente a relevância do consentimento, dos *cookies* e dos termos de uso que são gerados automaticamente: a sede da empresa e o local de registro ou de seus servidores podem impactar diretamente a jurisdição competente e a legislação que deve ser aplicada[166].

Tudo isso ganha novos contornos quando se considera que, hoje, muitos dados estão armazenados em nuvem (*cloud)*, o que revela, em verdade, a possibilidade de flexibilidade na definição da jurisdição competente[167].

É certo que, em casos envolvendo danos transnacionais que tenham ocorrido por meio da internet, existe competência internacional concorrente quando o réu, qualquer que seja sua nacionalidade, estiver domiciliado no Brasil, quando a obrigação aqui tenha que ser cumprida ou quando o fundamento seja fato ocorrido ou praticado no Brasil (art. 21 do CPC).

Além disso, não competirá à autoridade judiciária brasileira o processamento e julgamento da ação quando houver cláusula de eleição de foro exclusivo estrangeiro em contrato internacional (art. 25 do CPC) e, aqui, claro, deverão ser observados todos os pontos acerca de contratos de adesão.

Ademais, não se pretende esgotar o tema, afinal, são muitos pontos e características próprias e relativas ao Direito Internacional. No entanto, é de rigor entender que existem conflitos e, com o crescimento exponencial da internet, cada vez mais se torna necessário diploma que trate do tema como um todo ou que configure integralidade com aqueles presentes no âmbito internacional.

---

[165] Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:
I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
II - a natureza dos dados;
III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
IV - a adoção de medidas de segurança previstas em regulamento;
V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
VI - outras circunstâncias específicas relativas à transferência.

[166] MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 205.

[167] Ibid., p. 225

Nesse sentido, vale mencionar o julgamento do RMS 66392-RS, julgado em 16/08/2022 pelo C. STJ, de relatoria do Min. João Otávio de Noronha, em que ficou estabelecido que empresas que prestam serviços de aplicação na internet, mas que estejam em território brasileiro, devem se submeter ao ordenamento jurídico pátrio, independentemente de possuírem filiais no Brasil ou realizarem armazenamento em nuvem. No caso, um professor de um colégio estava sendo investigado pela prática de assédio sexual contra suas alunas, conduta que estaria sendo praticada principalmente por meio das redes sociais Facebook e Instagram.

O juiz determinou que a empresa Facebook, sediada nos EUA, fornecesse os conteúdos das mensagens privadas; houve impetração de Mandado de Segurança em face de tal determinação, entendendo que o fornecimento do material dependeria de cooperação internacional. O STJ não deu provimento ao recurso, pois o fato de estar sediada no exterior não pode eximir a empresa do cumprimento de leis e decisões judiciais, já que disponibiliza seus serviços para usuários que se encontram no Brasil[168]. Assim constou:

> CONSTITUCIONAL, PENAL E PROCESSUAL PENAL. RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. INVESTIGAÇÃO CRIMINAL. QUEBRA DE SIGILO TELEMÁTICO DOS INVESTIGADOS. PROVEDORA DE APLICAÇÃO. RECURSO DE FORNECIMENTO DE DADOS ARMAZENADOS EM SEUS SERVIDORES. UTILIZAÇÃO DE COOPERAÇÃO JURÍDICA INTERNACIONAL. DESNECESSIDADE. CRIME PRATICADO EM TERRITÓRIO NACIONAL, ATRAVÉS DE SERVIÇO OFERECIDO AOS USUÁRIOS BRASILEIROS. IRRELEVÂNCIA DE A PROVEDORA OPTAR PELO ARMAZENAMENTO DOS DADOS EM NUVEM. APLICAÇÃO DE MULTA DIÁRIA PELO DESCUMPRIMENTO. PROPORCIONALIDADE E RAZOABILIDADE. DESPROVIMENTO DO RECURSO ORDINÁRIO.
> 1. Empresas que prestam serviços de aplicação na internet em território brasileiro devem necessariamente se submeter ao ordenamento jurídico pátrio, independentemente da circunstância de possuírem filiais no Brasil.
> 2. O armazenamento em nuvem é estratégia empresarial que não interfere na obrigação de observância da legislação brasileira quando o serviço é prestado em território nacional.
> 3. A recalcitrância injustificada no cumprimento de decisão judicial atrai a imposição de multa como penalização da prática de ato atentatório à dignidade da Justiça.
> 4. Não há falar em excesso quando o valor fixado para a multa diária obedece aos parâmetros da razoabilidade e da proporcionalidade, guiado pela notória capacidade econômica da impetrante.
> 5. Recurso ordinário desprovido.
> [...]
> O que se espera de empresas que prestam serviço no Brasil é o fiel cumprimento da legislação pátria e cooperação na elucidação de condutas ilícitas, especialmente quando regularmente quebrado por decisão judicial o sigilo de dados dos envolvidos. Acrescento que o armazenamento em nuvem, estrategicamente utilizado por diversas empresas nacionais e estrangeiras, possibilita que armazenem dados em todos os

[168] CAVALCANTE, Márcio André Lopes. Facebook Inc, mesmo estando situada nos EUA, deve cumprir ordens judiciais para fornecimento de dados independentemente de pedido de cooperação jurídica internacional**. Buscador Dizer o Direito,** Manaus. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/8eab914c88e95773ea769310350ad7cb. Acesso em: 24 out. 2024.

> 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 [...][169].

São diversos parâmetros que devem ser observados visando sempre assegurar a proteção de dados pessoais durante todo o tratamento de dados.

2.5 LGPD PENAL

A LGPD, não obstante adote modelo de regulação de aplicação para empresas privadas e autoridades públicas, não adotou cautela acerca do tratamento de dados nas atividades de segurança pública e persecução penal, apenas destacando comando para criação de lei específica, que "deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei" (art. 4º, § 1º da Lei nº 13.709/2018).

Em outras palavras, a LGPD surge com o intuito de suprir a demanda acerca da proteção de dados. Ocorre que os artigos 3º e 4º do referido diploma vedam sua utilização em relação à segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais e, é nesse panorama, que se tem o Anteprojeto da LGPD Penal.

Dessa forma, a regulamentação da proteção de dados pessoais no âmbito da investigação e persecução penal se revela urgente, notadamente diante do inciso LXXIX do artigo 5º da CF/88 (com a promulgação da Emenda Constitucional 115/2022), que estabelece ser "assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Diante da lacuna quanto à lei específica, a Câmara dos Deputados, em 2019, criou uma comissão de juristas para redigir o anteprojeto de lei visando regular o tratamento de dados na esfera da investigação criminal.

Em novembro de 2020, foi apresentado o anteprojeto da Lei de Proteção de Dados para segurança pública e persecução penal, com influência da Diretiva 2016/680 da União Europeia e em legislações estadunidenses.

No anteprojeto, sobre as problemáticas centrais:

---

[169] BRASIL. Superior Tribunal de Justiça. **RMS nº 66.392**/RS (2021/0134439-7), Relator Ministro João Otávio de Noronha. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202101344397&dt_publicacao=19/08/2022. Acesso em: 24 out. 2024.

> O primeiro problema diz respeito à própria eficiência investigativa dos órgãos brasileiros, visto que a falta de adequação aos padrões internacionais de segurança quanto ao fluxo e ao tratamento de dados obsta a integração do Brasil com órgãos de inteligência e de investigação de caráter internacional (*v.g.*, INTERPOL) obstando o próprio acesso a bancos de dados e a informações relevantes, e coloca o uso de aplicações tecnológicas em segurança pública e a adoção de técnicas modernas de investigação sob questionamento de sua validade jurídica.
> Em segundo lugar, há um enorme déficit de proteção dos cidadãos, visto que não há regulação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos. Apesar do crescimento vertiginoso de novas técnicas de vigilância e de investigação, a ausência de regulamentação sobre o tema gera uma assimetria de poder muito grande entre os atores envolvidos (Estado e cidadão). Nesse contexto, o titular dos dados é deixado sem garantias normativas mínimas e mecanismos institucionais aplicáveis para resguardar seus direitos de personalidade, suas liberdades individuais e até a observância do devido processo legal[170].

Caso o anteprojeto se torne lei, haverá grande avanço normativo na justiça criminal brasileira. O artigo 1º elenca o objetivo da lei, qual seja, "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

Em sequência, o artigo 2º estabelece os fundamentos da proteção de dados, com o livre desenvolvimento da personalidade e o exercício da cidadania pelas pessoas naturais, autodeterminação informativa, o respeito à vida privada e à intimidade, liberdade de manifestação de pensamento, de expressão, de informação, de comunicação e opinião, presunção de inocência, confidencialidade e integridade dos sistemas informáticos pessoais, além da garantia do devido processo legal e ampla defesa e contraditório.

É evidente, em cenário global, a necessidade de ter a correta manipulação dessa prova, conferindo-lhe mais credibilidade e veracidade àquilo que se busca utilizar para instrução processual.

Nesse sentido, a Diretiva 680/2016 da União Europeia já regulou o tratamento de dados para fins de segurança pública e persecução penal. Destacam-se os seguintes pontos:

> (3) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A partilha e a recolha de dados pessoais registraram um aumento significativo. A tecnologia permite o tratamento de dados pessoais numa escala sem precedentes para o exercício de funções como a prevenção, investigação, deteção ou repressão de infrações penais e a execução de sanções penais.
> (4) A livre circulação de dados pessoais entre as autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de

[170] Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, elaborado por Grupo de Trabalho criado pela Câmara dos Deputados para sua formulação. Texto integral disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissaode-juristas-dados-pessoais-seguranca-publica/documentos/outrosdocumentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em: 13 dez. 2022.

> sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, a nível da União, e a sua transferência para países terceiros e organizações internacionais deverão ser facilitadas, assegurando simultaneamente um elevado nível de proteção dos dados pessoais. Este contexto obriga ao estabelecimento de um regime de proteção de dados pessoais sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras.
> [...]
> (7) É crucial assegurar um nível elevado e coerente de proteção dos dados pessoais das pessoas singulares e facilitar o intercâmbio de dados pessoais entre as autoridades competentes dos Estados-Membros, a fim de assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial. Para tal, o nível de proteção dos direitos e liberdades individuais no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais – incluindo a salvaguarda e a prevenção de ameaças à segurança pública – deverá ser equivalente em todos os Estados-Membros. A proteção eficaz dos dados pessoais na União exige não só que sejam reforçados os direitos dos titulares dos dados e as obrigações de quem trata dados pessoais, mas também que haja reforço dos poderes equivalentes para controlar e assegurar a conformidade com as regras de proteção dos dados pessoais nos Estados-Membros [...][171].

Ainda, extrai-se da exposição dos motivos como justificativas de sua existência:

> Desde logo, cabe destacar que foi opção do legislador não contemplar o tratamento de dados para segurança pública e investigação criminal no âmbito de aplicação da Lei Geral de Proteção de Dados (LGPD – Lei n. 13.709-2018), estabelecendo expressamente a necessidade de aprovação de lei específica para esse tema [...] Trata-se de um mandamento legal para legislar sobre a matéria, a partir da constatação de que está sujeita a ponderações específicas sobre o uso de dados pessoais e que expressa reivindicação da sociedade e das autoridades competentes para regulação do tema, surgida no processo de debate da própria LGPD.
> [...] a elaboração de uma legislação específica fundamenta-se na necessidade prática de que os órgãos responsáveis por atividades de segurança pública e de investigação/repressão criminais detenham segurança jurídica para exercer suas funções com maior eficiência e eficácia – como pela participação em mecanismos de cooperação internacional -, porém sempre de forma compatível com as garantias processuais e os direitos fundamentais dos titulares de dados envolvidos. Trata-se, portanto, de projeto que oferece balizas e parâmetros para operações de tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal, equilibrando tanto a proteção do titular contra mau uso e abusos como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações[172].

Além disso,

---

[171] UNIÃO EUROPEIA. DIRETIVA (UE) 2016/ 680 DO PARLAMENTO EUROPEU E DO CONSELHO - de 27 de abril de 2016 - relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/ 977/ JAI do Conselho (europa.eu), disponível em https://eur-lex,europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HR. Acesso em: 13 jan. 2023.

[172] Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, elaborado por Grupo de Trabalho criado pela Câmara dos Deputados para sua formulação. Texto integral disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissaode-juristas-dados-pessoais-seguranca-publica/documentos/outrosdocumentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em: 3 jan. 2023.

> [...] voltada para a investigação criminal e de segurança pública (LGPD-Penal), ou seja, o intuito deste anteprojeto é disciplinar os princípios, as diretrizes e as linhas mestras da proteção de dados no referido âmbito. Busca-se, portanto, harmonizar, de um lado, os deveres do Estado na prevenção e na repressão de ilícitos criminais, protegendo a ordem pública; de outro, assegurar a observância das garantias processuais e as prerrogativas fundamentais dos cidadãos brasileiros no que tange ao tratamento de dados pessoais para tais fins.
> Nesse sentido, tendo em vista a pretensão de introduzir normas gerais, esta 'LGPD-Penal' pretende complementar o microssistema legislativo de tratamento de dados para fins de segurança pública e de investigação criminal hoje existente em leis esparsas e voltadas sobretudo à regulamentação de quebras de sigilo no contexto processual penal (*v.g.*, disposições do Código de Processo Penal, da Lei das Interceptações Telefônicas e Telemáticas, da Lei Complementar n. 105, do Marco Civil da Internet, entre outras), modernizando-o à luz da nova realidade tecnológica e aprimorando-o com vistas a conferir maior segurança jurídica para todos os atores envolvidos[173].

Ainda, considerando como as tecnologias afetam os direitos fundamentais, o anteprojeto dispensou especial atenção direcionando um capítulo inteiro para sua regulamentação. Nesse sentido, o artigo 41, caput e § 1º, *in verbis:*

> A utilização de tecnologias de monitoramento ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados por autoridades competentes dependerá de previsão legal específica, que estabeleça garantias aos direitos dos titulares e seja precedida de relatório de impacto de vigilância.
> § 1º Para fins de avaliação do risco, deve-se considerar, pelo menos:
> I – a natureza dos dados pessoais envolvidos;
> II – as finalidades específicas do tratamento;
> III – a quantidade de agentes de tratamento de dados envolvidos;
> IV – a quantidade de titulares de dados potencialmente atingidos;
> V - se é utilizado algum tipo de nova tecnologia;
> VI – a possibilidade de tratamento discriminatório; e
> VII – as expectativas legítimas do titular de dados.

Também disciplina limites para o compartilhamento de dados entre as autoridades públicas:

> Art. 45, § 1º. Ressalvadas as hipóteses legais, é vedado o compartilhamento direto e contínuo de bancos de dados que contenham dados pessoais estabelecidos no âmbito de atividades de segurança pública com órgãos responsáveis pela persecução penal, exceto:
> I – nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei;
> II – para investigação ou processo criminal específico.

[173] Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, elaborado por Grupo de Trabalho criado pela Câmara dos Deputados para sua formulação. Texto integral disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissaode-juristas-dados-pessoais-seguranca-publica/documentos/outrosdocumentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em: 15 jan. 2023

Assim, a legislação atua em defesa dos indivíduos que fornecem informações, impedindo qualquer forma de discriminação e exigindo a análise contínua dos efeitos das ações de vigilância. Com a sua aplicação, certamente haverá melhorias nos procedimentos para garantir que causem o mínimo impacto negativo para aqueles que estão sendo investigados.

Dessa forma, a proposta de lei garante uma defesa significativa dos dados dos suspeitos, ao proibir a divulgação injustificada e excessiva de informações dos indivíduos, o que diminui a violação dos direitos à privacidade e à intimidade.

Neste momento, o Projeto de Lei está sob análise na Câmara dos Deputados aguardando um parlamentar para formalmente apresentá-lo e transformá-lo em Lei. Após essa etapa, o projeto seguirá os procedimentos habituais do processo legislativo, passando pela avaliação de diversas comissões, votação, envio ao Senado e aprovação do Presidente. Não se pode prever o tempo que levará para que o Anteprojeto se torne de fato uma lei; no entanto, é fato que é necessária uma legislação que proteja dados nas áreas de segurança pública e investigação criminal.

2.6 POLÍTICA PREVENTIVA NO AMBIENTE CIBERNÉTICO: A (IM)POSSIBILIDADE DE MONITORAMENTO

O direito penal e a lei adjetiva nada mais são do que reflexos da sociedade nos quais inseridos e, por tal razão e diante de novas tecnologias, a discussão revela-se imprescindível para que a instrução criminal – e eventual condenação – siga em consonância com os basilares constitucionais.

Urge a necessidade de análise no âmbito internacional, haja vista que o cruzamento de dados é uma realidade iminente, não apenas em crimes propriamente virtuais, mas qualquer infração.

Hoje, é evidente que o uso das redes sociais sugere a possibilidade de monitoramento; algoritmos analisam as pesquisas, coletando dados. No entanto, é necessária uma discussão sobre a possibilidade de utilização de tais dados no que tange aos princípios constitucionais, afinal, como isso será utilizado é o ponto que deverá ser detidamente analisado.

Mais que isso: a retirada de determinado conteúdo da internet pode resvalar em possíveis investigações. Vê-se que as características da prova digital (que serão à frente analisadas) sempre necessitam de uma análise sob tais perspectivas pois, novamente, se está lidando com provas cuja volatilidade e dispersão são evidentes.

Dessa forma, trabalhar com tais fatos utilizando os modelos tradicionais culmina em ineficiência da proteção do bem jurídico tutelado.

O que se pretende, pois, é entender como o monitoramento facilitaria a identificação de eventuais infratores pois a preservação do anonimato não traz vantagens, podendo comprometer a confiabilidade das informações disponíveis on-line, algo que já acontece, em parte devido à incerteza das fontes em determinadas circunstâncias. Na verdade, o anonimato apenas beneficia indivíduos que exploram a internet para propósitos duvidosos[174].

A questão que se traz é: quando se fala na necessidade de combate a algumas formas de criminalidade, com enfrentamento à criminalidade sem rosto e organizada, com bens difusos e coletivos, e macro (lavagens de capitais e crimes contra o sistema financeiro, por exemplo) é possível ainda entender pela intervenção mínima?

E ainda: poder-se-ia mencionar um papel do Direito Penal prospectivo ou antecipatório, visando evitar a lesão?

Ao observar a questão de crimes cometidos por meio da internet, a questão da prova e os direitos e garantias constitucionais, o debate sobre ser o Direito Penal sempre *ultima* ou *prima ratio* é necessário.

Esses novos meios de mídia convidam a refletir um pouco sobre esses pontos, sem significar a adoção de direito penal do inimigo[175], mas, sim, entender que a magnitude de determinados bens e interesses exige essa atuação prospectiva e não retrospectiva.

O Direito Penal Econômico acaba trabalhando, por si só, com elementos próprios de atuação prospectiva. Nesse sentido, não se há de falar em Direito Penal divorciado de outras medidas (administrativo sancionador, direito de intervenção); ao contrário, é entender que o direito administrativo sancionador, por exemplo, pode ser suficiente em alguns casos, mas, em outros, não.

A questão vai além, já que no âmbito empresarial a guarda e o fornecimento de dados (especialmente em investigação criminal) deve ser analisada considerando as consequências, como "quebra" e problemas financeiros à toda a sociedade.

Todo esse cuidado deve ser analisado, mas, como já mencionado, não é tarefa fácil: compreender todo o sistema e como tais questões devem ser decididas e analisadas para além

---

[174] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 85.

[175] Conforme Rafael Barros, "Para Jakobs, o inimigo é aquele que desafia as convenções da sociedade como estabelecidas e, dessa forma, ameaça a estrutura estatal buscando a destruição. Por não respeitar os regramentos próprio do estado democrático, esse indivíduo não faz jus aos direitos e garantias fundamentais aplicáveis aos cidadãos" (BARROS, Rafael. Entenda a teoria do direito penal do inimigo no Brasil. **Aurum**, 12 jun. 2023. Disponível em: https://www.aurum.com.br/blog/direito-penal-do-inimigo/. Acesso em 12 out. 2024.)

do exame das normas elencadas ganha novos contornos notadamente se considerada a tecnologia presente.

Outro ponto que o Direito Penal deve se ocupar dentro desse aspecto é a possibilidade de punição de atos preparatórios, a depender da magnitude do bem jurídico tutelado. Assim, outro tópico de debate surge para discussão: a depender da lesão, pode-se falar em intervenção máxima? Afinal, no âmbito empresarial, o caráter difuso encontra-se justamente na movimentação da economia, que afeta não apenas o território nacional, mas também outros países (o caráter transnacional é evidente e cada vez mais comum diante da internet, com a possibilidade de integração mundial).

O que se denota é que no combate à criminalidade econômica, o uso de preceitos e valores aplicados à ordinária pode não ter eficácia.

Não se pretende esgotar o tema, mas essas questões são pontos de partida para a compreensão de que se vive em uma nova era (a digital), que deve ser considerada em diversos campos, notadamente na investigação criminal e na colheita de provas.

3 PROVA DIGITAL: O NOVO PILAR DA EVIDÊNCIA JURÍDICA

3.1 FUNDAMENTOS E PERSPECTIVAS

Após conceituar a prova dentro da teoria geral e analisar o contexto dos direitos fundamentais que permeiam o tema, é de rigor avançar na definição da evidência digital, abordando suas características, os princípios que a norteiam e a questão da autenticidade e integridade das provas, enfatizando a importância da cadeia de custódia para assegurar a validade e sua integridade processual.

Vale destacar, inicialmente, que provas digitais não são apenas em crimes digitais, mas em delitos comuns também.

Pois bem.

Denise Vaz conceitua prova digital como "os dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias"[176].

Hodiernamente, a produção de provas não se limita apenas ao formato físico, alterando assim a própria dinâmica do direito processual. Dessa forma, as evidências digitais surgem como avanço tecnológico, possibilitando o acesso a meios de prova que antes não eram viáveis, inclusive facilitando o trabalho de investigadores e partes envolvidas no processo, contribuindo para maior agilidade.

A respeito do desenvolvimento tecnológico, a partir do século XX alcançou níveis extraordinários, com a criação da rede mundial de computadores até que passasse a se fazer presente em todas as relações[177].

Hoje, todos estão inseridos no ambiente virtual (aplicativos e redes interligadas) e esse espaço on-line é bastante diversificado e está em constante mudança, com o surgimento de novas ferramentas e oportunidades, o que ocorre a uma velocidade impressionante. Essa evolução contínua possibilita uma ampla variedade de atividades, que vão desde a troca de informações e o comércio on-line até a expansão das opções de entretenimento e ensino[178].

---

[176] VAZ, Denise Provasi. **Provas Digitais no Processo Penal:** Formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade de São Paulo, São Paulo, 2012, p. 63.
[177] Ibid., p. 18.
[178] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed. São Paulo: Revista dos Tribunais, 2024, p. 29.

E, por tal razão, as relações sociais migraram para o meio eletrônico e, como consequência, há uma espécie de "digitalização dos conflitos". Assim, o exame eletrônico é a forma de comprovar a existência de um evento ocorrido no ambiente on-line ou que utiliza a internet como forma de evidenciar um determinado acontecimento.

Denise Vaz ressalta que:

> Houve, assim, a substituição, em grande medida, de meios tradicionais de expressão por novos meios tecnológicos. Apenas como ilustração, pode-se citar que: os documentos anteriormente redigidos e arquivados em papel tornaram-se eletrônicos; as músicas foram transferidas do disco de vinil e da fita cassete para o formato digital; as fotografias deixaram de ser registradas em filme para também assumirem o formato digital; do mesmo modo, a captação de imagens em vídeos; e ainda a comunicação por cartas, bilhetes, telegrama, telefone, foi transmudada em mensagens eletrônicas de texto, *e-mails,* sistemas VoIP, dentre outros.
> Tais transformações caracterizam uma revolução tecnológica, a "revolução informacional", comparável, por seus efeitos, à Revolução Industrial. Ela deu ensejo à denominada "sociedade de informação" ou "sociedade pós-industrial", formada na segunda metade do século XX[179].

O que se vê é que os números crescem. Os resultados realizados pelo Instituto de Geografia e Estatística (IBGE) indicaram que o equipamento mais utilizado para o uso da internet em 2022 foi o telefone móvel (98,9%), sendo que o percentual de frequência com que utilizavam a internet todos os dias era de 93,4%. Além disso, a proporção de pessoas com 10 anos ou mais passou de 84,7% em 2021 para 87,2% em 2022[180].

Em 2023, os números aumentaram, inclusive acerca do percentual de idosos que utilizam a internet[181].

Como consequência, cada vez mais são gerados nesse espaço registros variados por meio de dispositivos eletrônicos, processados e salvos em formato digital, seguindo a lógica de zeros e uns. Nesse sentido:

> [...] suportes físicos em que se encontram armazenados os dados – computadores, pen drives, CDs, DVDs, telefones celulares, aparelhos de MP3, as urnas eletrônicas, câmeras de vídeo ou fotográficas, etc. Do mesmo modo, com relação aos arquivos

---

[179] VAZ, Denise Provasi. **Provas Digitais no Processo Penal:** Formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade de São Paulo, São Paulo, 2012, p. 19.

[180] BELANDI, Caio. 161,6 milhões de pessoas com 10 anos ou mais de idade utilizaram a Internet no país, em 2022. **AGÊNCIA IBGE**, 09 nov. 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=Para%2066%2C1%25%20dos%20idosos,2021%20(84%2C4%25. Acesso em: 03 mar. 2024.

[181] NERY, Carmen. Em 2023, 88,0% das pessoas com 10 anos ou mais utilizaram Internet. **AGÊNCIA IBGE,** 16 ago. 2024. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet. Acesso em: 31 out. 2024.

> neles contido – imagens, vídeos, músicas, documentos de texto, correspondências eletrônicas, páginas de sites, dentre outros. Para a aquisição dessas fontes, são utilizados vários meios de pesquisa, como busca e apreensões, interceptações, infiltrações em redes ou suportes, os quais podem ser entendidos como meios de obtenção de provas digitais. Posteriormente, ocorre a introdução das fontes no processo, com a perícia e a prova documental, que constituem os meios de produção da prova digital. Os elementos obtidos das fontes digitais, em conjunto com os demais elementos do processo, conduzem então ao resultado probatório, por meio da verificação das asserções feitas pelas partes[182].

A prova digital possui natureza de fonte de prova e, a partir dela, porquanto assemelha-se a um documento, será possível extrair as informações relevantes para o processo penal[183].

Assim, valorar a prova digital da mesma forma que a física não se revela a melhor técnica, considerando suas peculiaridades, conforme elucida Dario José Kist:

> [...] um dos campos no qual é perceptível de forma contundente essa diferença é o da obtenção de meios de prova: a clássica busca e apreensão deverá ser uma pesquisa informática tendente a identificar, no interior de sistemas telemáticos, dados dessa natureza e que tenham potencial probatório para, na sequência, proceder à sua apreensão; e essa pesquisa poderá revelar que os dados buscados encontram-se armazenados em sistema informático em outro país, o que movimentará uma grande gama de questões acerca da aplicação territorial ou extraterritorial das leis do país que está promovendo a pesquisa; as regras jurídicas desenvolvidas para o trato da interceptação da correspondência postal de pouca valia terão quando houver necessidade de apreender um correio eletrônico/e-mail; a apreensão de um dispositivo informático, a exemplo de um smarthphone, em contexto de busca pessoal, e diante da probabilidade de em sua memória estarem armazenados dados que, eventualmente, sejam relevantes para a prova de um crime, põe a questão sobre os requisitos para que o acesso promovido pela polícia seja legítimo; se eventualmente o acesso ao referido dispositivo informático estiver condicionado a uma chave/senha, põe-se a questão sobre eventual obrigação do indivíduo visado em colaborar com a investigação fornecendo a citada senha[184].

Portanto, os avanços tecnológicos são cada vez mais irrefreáveis na atual sociedade, o que tem levado a um aumento significativo na utilização de dados digitais como evidências em processos criminais, ou seja, as chamadas provas digitais.

No entanto, sua análise não é tão simples, afinal, existem equipamentos de processamento de dados, estruturas físicas, redes conectadas o que possibilita inclusive a evasão de modo muito mais fácil. Nesse sentido, pode-se pensar que documento físico (papel) existe ou não. É algo verdadeiramente palpável; sua destruição, portanto, é também evidenciada aos olhos, ao contrário do que ocorre em um documento digital afinal, ainda que se destrua (delete) o arquivo, ele ainda pode subsistir em outros dispositivos ou até mesmo em nuvem (*cloud*

---

[182] VAZ, Denise Provasi. **Provas Digitais no Processo Penal:** Formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade de São Paulo, São Paulo, 2012., p. 60-61.
[183] Ibid., p. 63.
[184] KIST, Dario José. **Prova Digital no Processo penal**. Leme, SP: JH Mizuno, 2019, p. 55-56.

system). Além disso, sua manipulação também pode ocorrer e, todos esses fatos não são tangíveis, evidenciados a olho nu. Dessa forma, estando diante de provas diferenciadas, faz-se necessária análise também diversa, com instrumentalidade para tanto.

A tecnologia por trás dos dados é complexa:

> Em um *datacenter*, que consiste em ser um local preparado para comportar computadores com alto volume de processamento de dados, o funcionamento de um "servidor" não é tão diferente de um computador doméstico. Porém, geralmente, esse tipo de computador possui peças melhor adaptadas para um funcionamento contínuo e *softwares* mais técnicos, para que atendam milhões de solicitações de forma rápida. Ao acessar um *website*, o seu computador faz uma requisição *via comunicação de rede* para o servidor em questão, que usará sua memória estática para buscar e disponibilizar as informações necessárias. Isso ocorre juntamente com a operação de seu CPU e memória RAM, interligados por uma placa-mãe, que respondem com outros dados ao usuário de internet. É comum que aplicativos de celular também recorram a servidores na internet para gravar ou consultar informações, processando-as remotamente ou permitindo que você acesse o aplicativo de outro celular sem perder seus dados.
> Portanto, são sempre computadores trocando informações entre si, e se você entende como funciona um computador doméstico, você sabe também como funciona um computador especializado como um "servidor de dados".
> [...] Ao se conectar em uma rede de dados, seu computador troca informações com outros computadores ou servidores, podendo obter informações a partir de uma fonte externa. Nessa troca, não há necessariamente um armazenamento das informações; há, porém, a possibilidade de interceptá-las ou gravá-las, verificando o conteúdo trocado no momento em que ocorrem.
> [...] Em resumo, temos dados em seu estado original, nas memórias dos computadores, servidores, celulares e outros dispositivos, ou recebidos em interfaces de redes via cabo, rádio e outros meios.
> Dando um passo à frente, essas peças de computador não são feitas para organizar e processar os dados para determinado objetivo específico, necessitando de "softwares" programados para determinadas funções que se deseja obter[185].

Além disso, não se pode olvidar que a forma que os recursos são usados mudou – e assim continuará acontecendo. Nesse sentido:

> É cada vez mais comum que os dados não fiquem mais armazenados no computador do usuário, sendo gravados e consultados a partir da Rede Mundial de Computadores, desde *websites* como o Wikipédia, que sempre estão disponíveis para consultas esporádicas, até serviços de armazenamento em nuvem, para manter seus arquivos salvos e seguros. Muito da vida e trabalho dos usuários hoje estão na nuvem (ou *cloud*). Tal situação abre outra fonte de dados no meio digital: *dados gravados em servidores da internet, externos ao dispositivo do usuário*. O acesso direto aos equipamentos e memórias envolvidos na computação em nuvem é particularmente difícil. Isso porque os equipamentos são configurados para atuar de forma compartilhada, replicada e redundante.
> Sendo assim, as informações de um determinado usuário podem estar divididas entre vários equipamentos ou sendo movidas sob demanda em questão de segundos para garantir a disponibilidade do serviço. Nesses casos, há praticamente uma impossibilidade de acessar fisicamente o equipamento para periciar informações, sendo

[185] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed. São Paulo: Revista dos Tribunais, 2024, p. 31-32.

> o acesso via conexão de dados o único caminho viável para se obter as informações necessárias[186].

Dessa forma, o que se vê é que a celeridade e praticidade da tecnologia também traz em sua essência uma existência híbrida – que até pouco tempo poderia ser experimentada apenas por meio de ficções científicas – de modo que a vida não se alterna mais entre a conexão ou não, pois todos estão interligados por meio de smartphones, câmeras, veículos com integração. E é essa "matrix" que faz com que a prova digital seja estudada e colhida com observância de suas particularidades.

3.2 AS ORIGENS DA PROVA DIGITAL: DIREITO PROBATÓRIO DE TERCEIRA GERAÇÃO

Importante destacar a evolução das gerações do direito probatório e, consequentemente, seus reflexos na persecução penal. No decorrer da história, com conquistas de direitos e garantias fundamentais, a atuação do Estado foi restrita, diante da democracia, sistema acusatório e constituição garantista.

E, lastreada em precedentes da Suprema Corte norte-americana, presentes marcos históricos que apontam a existência de gerações probatórias.

Nesse sentido, João Biffe e Joaquim Leitão Júnior destacam que:

> A divisão das gerações de direito probatório encontra seu nascedouro nos precedentes Olmstead (1928), Katz (1967) e Kyllo (2001), nos quais a Suprema Corte Norte-Americana decidiu em quais casos incidiria a proteção conferida pela 4ª emenda à Constituição dos Estados Unidos da América, tornando-se assim necessária a expedição prévia de ordem judicial de busca e apreensão para a obtenção lícita das provas[187].

No direito probatório de 1ª geração, tem-se a teoria proprietária (*trespass theory*), no precedente *Olmstead v. United States*, de 1928. Nesta, foi discutida a validade de prova decorrente de interceptação telefônica que ocorreu sem autorização judicial por acesso direto à empresa responsável pelo serviço, que estava localizada em espaço público – de tal sorte que não houve invasão ao domicílio. Dessa forma, o ponto fulcral da discussão era acerca da licitude

---

[186] Ibid., p. 34-35.

[187] BIFFE JÚNIOR, João; LEITÃO JÚNIOR, Joaquim**.** O acesso pela polícia a conversas gravadas no Whatsapp e as gerações probatórias decorrentes das limitações à atuação estatal. **Genjurídico**, 12 ago. 2016. Disponível em: https://blog.grupogen.com.br/juridico/areas-de-interesse/penal/o-acesso-pela-policia-a-conversas-gravadas-no-whatsapp-e-as-geracoes-probatorias-decorrentes-das-limitacoes-a-atuacao-estatal/. Acesso em: 06 jun. 2024.

dessa prova, e a Suprema Corte norte-americana entendeu que a investigação ocorreu de forma idônea, vez que não houve ingresso à propriedade do acusado; em outras palavras, não poderia haver uma interpretação alargada do constante na quarta emenda[188], de tal sorte que a proteção constitucional seria aplicada apenas a áreas demarcáveis, o que não ocorre no caso de captação de imagem e voz, mesmo aquela realizada por meio de interceptação telefônica.

Em suma, a proteção era direcionada à inviolabilidade de comunicações e privacidade em residências, havendo, portanto, uma forma mais limitada de salvaguarda (por isso teoria proprietária).

Acerca do caso, Danilo Knijnik explica que:

> [...] julgado em 1928 pela Suprema Corte americana, Olmstead teve conversas telefônicas interceptadas pela inserção de um equipamento diretamente na fiação da empresa telefônica e na via pública. Os investigadores não haviam invadido, penetrado ou adentrado no domicílio, na propriedade ou nos pertences de quem quer que fosse. E o sinal de `voz` que corria pelos fios da companhia telefônica não era uma **coisa**.
> Chamada a apreciar a alegação de que a prova seria ilícita, pois realizada sem mandado judicial, a Suprema Corte concluiu que a ação policial não havia "penetrado em qualquer propriedade do acusado", e que a correta interpretação da 4ª Emenda não poderia dar-se de forma a "alargá-la para além do conceito prático de pessoas, casas, papeis e pertences" ou "para aplicar buscas e apreensões de forma a proibir escutar ou observar".
> Esse precedente consagrou o que a doutrina convencionou chamar de "trespass theory" ou "teoria proprietária": a proteção constitucional estender-se-ia apenas para as áreas tangíveis e demarcáveis, exigindo a entrada, o ingresso e a violação de um espaço privado ou particular, o que, na espécie, efetivamente não havia ocorrido, dado que nenhuma propriedade de Olmstead fora devassada pela autoridade. Neste inicial da trilogia, surge uma interpretação constitucional protetiva de coisas, objetos e lugares[189].

Posteriormente, surge o direito de 2ª geração, no precedente *Katz v. United States*, em 1967, quando a polícia, também sem invadir propriedade privada, realizou captação de voz em cabine telefônica. Num primeiro momento, aplicados os precedentes firmados no caso Olmstead, mas, ao chegar na Suprema Corte, houve alteração do posicionamento, entendendo que a proteção à intimidade e privacidade não permaneceriam limitadas às áreas tangíveis e demarcáveis. Nesse sentido, explica Knijnik:

---

[188] A Quarta Emenda estabelece que "O direito das pessoas de estarem seguras em suas pessoas, casas, papeis e pertences, contra buscas e apreensões não razoáveis, não deve ser violada e nenhum mandado deve ser emitido, mas por causa provável, apoiado por juramente ou afirmação, e particularmente descrevendo o local a ser revistado e as pessoas ou coisas a serem apreendidas" (NATIONAL CONSTITUTION CENTER. **Fourth Amendment:** Search and Seizure. Disponível em: https://constitutioncenter.org/the-constitution/amendments/amendment-iv. Acesso em: 11 jun. 2024).

[189] KNIJNIK, Danilo. A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI. **Revista da Escola da Magistratura do TRF da 4ª Região**, ano 2, número 4. Porto Alegre/RS, 2016. Disponível em: https://www.trf4.jus.br/trf4/upload/editor/2019/bnu_05-a-trilogia.pdf. Acesso em: 4 jun. 2024, p. 86.

> Passados 39 anos, chegara a vez de apreciar outra iniciativa policial: baseada em Olmstead, a polícia, sem invadir absolutamente nada, instalou um equipamento capaz de gravar a voz do usuário de uma cabine telefônica. Aparentemente, a técnica adequava-se ao *leading-case* Olmstead. Afinal, o telefone era público, nenhum "trespass", invasão ou ingresso teria sido perpetrado pelos oficiais em propriedade ou espaços do acusado e, ainda assim, a voz do interlocutor, que também não era uma coisa, fora "apreendida". Todavia, confrontada com tal prova, a interpretação pendeu para o outro lado da margem, e Katz teve melhor sorte que Olmstead.
> Com efeito, em Katz v. United States, o tribunal de apelação havia admitido a referida prova, asseverando justamente à luz da teoria proprietária, que "não houve qualquer violação à 4ª Emenda, pois inexistente qualquer ingresso físico na área ocupada pelo acusado". Mas a *ratio* de Olmstead, e a teoria que lhe era subjacente, não resistiu à pressão dos tempos e à eloquência dos resultados: a Suprema Corte viria a entender, nesse momento, que a polícia havia realizado uma "busca", dependente da obtenção de um mandado judicial, sendo nula, portanto, a diligência.
> A novidade ficou por conta da seguinte *ratio*: "a 4ª Emenda regula não apenas a busca de itens tangíveis, mas estende-se, também, para a gravação de declarações orais [...]". Girando o foco da proteção constitucional, Katz concluiu no sentido de que, "**uma vez que a 4ª Emenda protege pessoas, mais que lugares, sua finalidade não pode ser frustrada pela presença ou ausência de uma intrusão física em qualquer compartimento fechado**. A doutrina proprietária (*trespass theory*) de Olmstead v. US, 227 US 438; e Goldman v US, 316 US 129 não será a regra". A isso, acrescentou o tribunal que, "muito embora o monitoramento, neste caso, possa ter sido tão sutilmente circunscrito, a poder ser constitucionalmente autorizado antecipadamente, ele **não fora conduzido conforme a exigência de um mandado**"[190].

Além disso, acrescenta que:

> Nessa transição Olmstead-Katz, **o âmbito de proteção constitucional**, como visto, **migrou de coisas**, **lugares e pertences para pessoas e suas expectativas de privacidade**. Foi assim que um número muito maior de ocorrências, não atendidas pela teoria proprietária, foi posto sob a custódia da 4ª Emenda da Constituição americana. Basicamente, a evolução introduzida por Katz, de extrema importância, implicou o afastamento da teoria proprietária como expressão integral da proteção constitucional, com a introdução de um teste bem mais complexo, formado por duas indagações: primeiro, se há uma expectativa subjetiva real e efetiva de privacidade; segundo, se a sociedade está disposta a reconhecer essa expectativa como razoável, ou seja, se está disposta a confirmar a pretensão do sujeito real. Com base em tais critérios, por exemplo, afastou-se a arguição de ilicitude de prova consistente em voo rasante sobre o jardim da residência do investigado, que acabou por comprovar, mediante utilização de câmeras sofisticadas, o cultivo de *cannabis sativa*. Embora existente uma expectativa do sujeito de não ser bisbilhotado do ar, fato é que a sociedade não reconhece uma proibição dos passageiros de uma aeronave de contemplarem a paisagem e, se for o caso, constatarem detalhes importantes da vida de terceiros (original sem destaque)[191].

[190] KNIJNIK, Danilo. A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI. **Revista da Escola da Magistratura do TRF da 4ª Região**, ano 2, número 4. Porto Alegre/RS, 2016. Disponível em: https://www.trf4.jus.br/trf4/upload/editor/2019/bnu_05-a-trilogia.pdf. Acesso em: 4 jun. 2024, p. 86/87.
[191] Ibid., p. 87.

Dessa forma, no direito probatório de segunda geração, observa-se proteção com maior abrangência, pois incluídas as comunicações telefônicas mesmo decorrentes de ambiente público.

Por fim, surge o direito probatório de 3ª geração, no precedente *Danny Lee Kyllo v. United States*, de 2001. Neste caso, havia suspeita de plantação de *cannabis sativa* dentro da residência de Danny, porém, ausente lastro probatório suficiente a fundamentar requerimento de expedição de mandado de busca e apreensão judicial.

Diante disso, os investigadores tiveram a ideia de utilizar equipamentos para aferir a temperatura térmica do local – afinal, para o cultivo da referida planta, seria necessário o uso de lâmpadas de alta intensidade. O que se tem, portanto, é a utilização de provas invasivas que permitissem colher elementos suficientes, mas, diferentemente dos demais precedentes, não haveria discussão quanto à invasão do interior da residência ou espionagem do local. Referida prova foi admitida. Dessa forma:

> [...] o argumento utilizado pela acusação, como já referido, consistiu basicamente na circunstância de que a prova respeitava de forma plena a doutrina Katz: não tinha havido **busca de espécie alguma,** pois radiações caloríficas não são coisas nem pertences; no duplo teste de Katz – vale dizer, se Kyllo tinha real expectativa de privacidade e se a sociedade reconhecia essa expectativa como razoável -, a solução também não lhe era favorável, porquanto, segundo argumentou o acórdão recorrido do 9º Circuito, Kyllo não fez absolutamente nada para conter a emanação de calor de sua propriedade, demonstrando não ter real expectativa de privacidade. E parece pouco crível que a sociedade reconheceria sua pretensão como razoável, pois o Agema Thermovision 210 (equipamento utilizado no caso) não revelara detalhes íntimos de sua vida, caso em que talvez a conclusão pudesse ser outra.
> Ainda assim, algo não parecia justo na espécie. Kyllo, de certa forma, estava "escondido" nos domínios de sua casa. Ele não cultivara maconha no seu jardim. E o Agema Thermovision captou algo que pessoa alguma conseguiria captar. De alguma forma, a tecnologia foi lá onde os sentidos não chegavam. Aqui, algo além de uma observação havia ocorrido.
> Ao examinar o caso, o Justice Scalia começa por dizer que, efetivamente, a 4ª Emenda protege as pessoas contra "buscas" sem mandado. Sem dúvida, com base na tradição da common law, admite-se, sim, a simples vigilância de alguém pela polícia, colhendo-se informações que os órgãos dos sentidos puderem, pois "os olhos não podem, pelas leis inglesas, ser acusados de uma invasão. E jamais se poderia exigir a um agente da lei fechar os olhos para o que assiste na via pública. Portanto, a simples observação visual, de fato, não representaria busca alguma[192].

Diante disso, é possível aferir que a prova digital tem aqui suas origens - na terceira geração dos direitos probatórios - já que decorre desse avanço da tecnologia.

Nesse sentido, Knijnik destaca que na decisão do referido precedente constou que:

---

[192] KNIJNIK, Danilo. A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI. **Revista da Escola da Magistratura do TRF da 4ª Região**, ano 2, número 4. Porto Alegre/RS, 2016. Disponível em: https://www.trf4.jus.br/trf4/upload/editor/2019/bnu_05-a-trilogia.pdf. Acesso em: 4 jun. 2024, p. 88-89.

> [...] nos dias de hoje [...] o "mundo virtual" da tecnologia integra a "realidade". E a materialidade das coisas, tal qual no passado entendida, não pode limitar o escopo e a abrangência da proteção constitucional outorgada às **pessoas**. Assim, a interpretação da 4ª Emenda, ao aludir a "**coisas**", "**pertences**", "**papeis**", "**lugares**", deveria sofrer uma atualização interpretativa, para além da doutrina Katz. Agora, o monitoramento "pela janela" vs "através da janela" encerrava uma distinção irrelevante, derruída pelo agigantamento da sofisticação, não mais podendo servir como marco divisório para o alcance da proteção constitucional (destaque no original)[193].

O que se vê, portanto, é a necessidade de entender a mudança em diversos pontos quanto à obtenção da prova, já que, de modo tangível, pode não haver qualquer violação, mas, num mundo cada vez mais híbrido – com interligação entre pessoa e tecnologia – é evidente a intervenção na esfera da liberdade de cada indivíduo.

Por essa razão, Danilo Knijnik ressalta que o avanço da tecnologia deve ser compatibilizado com as garantias constitucionais e "se os mecanismos probatórios mudaram, a interpretação jurídica tem de acompanhar, simetricamente, essa transformação"[194].

É evidente, portanto, que o avanço tecnológico determinou mudança na condução das investigações, afinal, existem novos meios de comunicação de dados e é diante dessa mudança que as formas de fornecimento de dados – notadamente aqueles inseridos na nuvem – devem ser estudados.

Nesse sentido:

> Depreende-se que, no direito probatório de primeira geração, houve uma proteção direcionada à inviolabilidade das comunicações telefônicas e a privacidade em residências de forma mais limitada, fixando a teoria proprietária.
> No direito probatório de segunda geração, a proteção progrediu de modo a englobar as expectativas de privacidade referente às comunicações telefônicas, ainda que derivadas de ação em ambiente público.
> Fechando a trilogia, o direito probatório de terceira geração proporcionou uma abrangência ainda maior, protegendo o indivíduo dos meios de obtenção de provas elevadamente tecnológicos e intromissivos da privacidade, incluindo a comunicação de dados em telefones celulares.
> Essa terceira geração probatória ganha atenção especial por se tratar da geração em que é contemporâneo ao presente momento, com o enfoque eminentemente tecnológico.
> É notada uma constante evolução da jurisprudência em uma árdua tentativa de acompanhar o ritmo de avanço das tecnologias e suas modificações na sociedade, tendo em vista que poder legislativo não consegue conferir às leis a mesma celeridade que o judiciário consegue promover na sua interpretação e aplicação prática, de forma a moldar às realidades atuais[195].

---

[193] KNIJNIK, Danilo. A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI. **Revista da Escola da Magistratura do TRF da 4ª Região**, ano 2, número 4. Porto Alegre/RS, 2016. Disponível em: https://www.trf4.jus.br/trf4/upload/editor/2019/bnu_05-a-trilogia.pdf. Acesso em: 4 jun. 2024, p. 89.
[194] Ibid., p. 94.
[195] FERNANDES, Robério Fernandes Júnior. A evolução e o impacto das gerações probatórias na persecução penal sob os influxos dos atuais mecanismos telefônicos. **Escola superior do Ministério Público do Ceará**, ano

A terceira geração do direito probatório foi tratado pelo STJ, no julgamento do HC 51.531, ao tratar de acesso dos policiais a aplicativos de celulares apreendidos, entendendo ilícita a "devassa de dados, bem como das conversas de whatsapp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial".

Aliás, no referido julgado é mencionado outro precedente: *Riley v. California*. Neste, David Leon Riley foi abordado, em 22/08/2009, pela polícia de San Diego com carteira de motorista vencida e, revistado seu veículo, foram localizadas duas pistolas. Na sequência, a polícia investigou seu telefone celular, sem qualquer mandado, e descobriu que ele era um membro de gangue envolvida em diversos assassinatos. A defesa alegou a ilegalidade das provas, argumentando violação à Quarta Emenda, alegação que foi inicialmente afastada, mas, posteriormente, acolhida pela Suprema Corte. Como constou, "concluiu que um mandado é necessário para acessar o telefone celular de um cidadão na hipótese de prisão em flagrante, haja vista "que telefones celulares modernos não são apenas mais conveniência tecnológica, porque o seu conteúdo revela a intimidade da vida. O fato de a tecnologia agora permitir que um indivíduo transporte essas informações em sua mão não torna a informação menos digna de proteção"[196].

Assim, considerando o contexto histórico até a CF/88, é possível concluir que esses meios digitais também estão salvaguardados na garantia de inviolabilidade e da intimidade, o que leva a entender a necessidade de maiores cuidados em sua obtenção e custódia.

3.3 CARACTERÍSTICAS: O QUE DEFINE UMA PROVA DIGITAL?

A prova digital possui características próprias, que impactam na abordagem, identificação e colheita; consequentemente, também denotam diferenças na investigação criminal[197].

Algumas características são elencadas acerca da referida espécie probatória, como: (i) imaterialidade; (ii) volatilidade; e (iii) dispersão. É imaterial pois, em sua essência, é formada

14, n. 1, jan.-jul., p. 11-30, 2022. Disponível em: https://revistaacademica.mpce.mp.br/revista/article/view/202/167. Acesso em: 27 out. 2024.

[196] BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso em Habeas Corpus nº 51531** – RO, 2014. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=59034141&num_registro=201402323677&data=20160509&tipo=3&formato=PDF. Acesso em: 11 jun. 2024.

[197] KIST, Dario José. **Prova digital no processo penal**. Leme, SP: HJ, Mizuno, 2019, p. 115.

por uma sequência de bits e está presente de forma independente de um suporte físico. Assim, embora os dados digitais tenham uma existência concreta, eles não podem ser fisicamente tocados; é volátil e frágil, justamente porque não existe suporte físico (daí a necessidade da manipulação de forma cuidadosa), afinal, podem desaparecer; e, por fim, dispersão porque a prova pode estar em locais diferentes, ainda que dentro de um mesmo sistema informático ou em dados armazenados em nuvem e em locais diversos[198].

Destaca Gustavo Badaró:

> [...] duas características são destacadas como mais relevantes: a desmaterialização e a dispersão dos elementos de prova.
> No que toca à sua "desmaterialização", não se trata de provas pensáveis como objetos físicos, dotados de uma evidente corporeidade. E é exatamente dessa impalpabilidade que decorre os caráteres de volatilidade e fragilidade da própria prova digital, razão pela qual há necessidade de uma maior preocupação com a possibilidade de falsificação ou destruição. Há, na prova digital, uma "congênita mutabilidade". Em suma, trata-se de fonte de prova que pode ser facilmente contaminada, sendo sua gestão muito delicada, por apresentar um alto grau de vulnerabilidade a erros[199].

Denise Vaz destaca que:

> De fato, a principal característica da prova digital reside no fato de se tratar de objeto imaterial (sequência numérica), que pode ser facilmente alterado, como também pode ser copiado e difundido, necessitando de um equipamento intermediário para ser acessado.
> Por outro lado, não se pode afirmar que não durabilidade seja característica de toda prova digital, pois os dados informáticos armazenados em dispositivos eletrônicos são submetidos a técnicas de preservação. De igual modo, os dados transmitidos em rede são captados e fixados em suportes eletrônicos, de forma a os tornar permanentes.
> A disseminação dos dados, pulverizados em diferentes ambientes eletrônicos tampouco constitui característica comum e essencial a toda prova digital. O objeto de interesse para a persecução penal pode se encontrar armazenado em um único dispositivo, em um só arquivo. No entanto, a dispersão corresponde a uma possibilidade, que deve ser considerada durante a investigação[200].

Assim, Vaz traz mais alguns elementos acerca da prova digital: (i) suscetibilidade de clonagem; e (ii) necessidade de intermediação de equipamento para ser acessada. O primeiro diz respeito à cópia do arquivo, permitindo a transferência a outros dispositivos e o segundo, à

---

198 KIST, Dario José. **Prova digital no processo penal**. Leme, SP: HJ, Mizuno, 2019, p. 118.

199 BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM,** ano 29, n. 343, jun. p. 7-9, 2021. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325/627. Acesso em: 31 out. 2024.

200 VAZ, Denise Provasi. **Provas Digitais no Processo Penal:** Formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade de São Paulo, São Paulo, 2012, p. 67.

necessidade de equipamento para processar a informação, vez que o dado (digital) trata-se de código[201].

Acerca do tema, Saad, Rossi e Partata destacam:

> O atributo "digital" não decorre da simples utilização de dispositivo informático no encaminhamento ou na produção do elemento de prova. Do contrário, quaisquer documentos poderiam ser classificados como provas digitais. Essa qualificação é relativa apenas ao próprio arquivo informático, pois liga diretamente o conteúdo da informação (que importa à persecução penal) à manipulação eletrônica de números. A capacidade representativa de fatos ou ideias vincula-se, portanto, a um processo interpretativo, que atribui um sentido humanamente compreensível a uma linguagem não natural.
> A prova digital, contrapondo-se às provas ditas analógicas, é marcada por características distintivas. A *imaterialidade*, por exemplo, diz respeito à "natureza impalpável" da prova, pois os dados em formato digital não são nada além de impulsos de corrente elétrica, aos quais se atribui um sentido informacional após um processo de interpretação de uma linguagem não natural. Por ser imaterial, aponta-se também a *volatilidade* como característica: os dados digitais são frágeis e podem sofrer variações (propositais ou involuntárias), bastando, para tanto, a simples modificação da sequência numérica que os compõe.
> As provas digitais também apresentam integral *desprendimento do suporte físico* onde estão registradas, de modo que as informações produzidas e/ou armazenadas podem ser transferidas para outros dispositivos ou formas de armazenamento sem perder sua essência. Esta característica liga-se diretamente com a *suscetibilidade de clonagem*, o que significa dizer que estes dados permitem a realização de cópias – fiéis, idênticas e infinitas – dos arquivos digitais, desde que se promova o espelhamento dos elementos coletados. Por fim, aponta-se a *necessidade de intermediação* de equipamento: como o dado digital é uma simples sequência numérica que, isoladamente, pouco significa para o ser humano, torna-se necessário o uso de equipamentos que processem essas informações e as disponibilizam em linguagem natural, compreensível ao ser humano[202].

Tais características evidenciam, em verdade, o cuidado necessário acerca de sua coleta, notadamente porque a legislação não evolui com a mesma velocidade que as tecnologias, o que denotam lacunas que, no caso concreto, culminam em verdadeiras atribulações práticas. No mais das vezes, na busca incessante para fazer cumprir o que já está disposto no ordenamento jurídico, pode acabar fulminando direitos já garantidos e, consequentemente, violar o processo com nulidade.

Dessa forma, um novo olhar deve ser lançado sobre a prova digital. Afinal:

> No cenário digital, temos preocupações diferentes com relação à sua confiabilidade, já que é um ambiente mais volátil e podem ocorrer situações em que um material pode ser fabricado ou modificado sem deixar vestígios suficientes para verificá-lo. Portanto, existe uma demanda por maior cuidado no processo de sua extração e

[201] Ibid., p. 69.
[202] SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda uma disciplina própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. **Rev. Bras. de Direito Processual Penal,** Porto alegre, v. 10, n. 3, e1071, set-dez. 2024. Disponível em https://revista.ibraspp.com.br/RBDPP/article/view/1071/547. Acesso em: 31 out. 2024.

> documentação, para que seja confiável e, sobretudo, corresponda com a realidade dos fatos [...][203].

Como mencionado, as provas digitais fazem parte do cotidiano: um smartphone possui mais informações sobre a vida privada dos indivíduos do que a própria casa, determinando, dessa forma, uma carga maior cuidado com privacidade[204].

Portanto, observadas as características, a maneira como essas evidências são coletadas, preservadas e, posteriormente, analisadas, será fundamental na análise das provas digitais e como o processo digital – embrionariamente analógico – pode se compatibilizar com esse universo.

Acerca do tema, Aury Lopes Jr. instiga a diversas indagações:

> Como as garantias fundamentais, de matriz analógica-iluminista até, podem (ou não) se efetivar nesse contexto? Ou seja, como falar em direito de não autoincriminação ou do contraditório efetivo, quando se tem diante de si um *smartphone,* por exemplo, que contém minhas fotos, ligações, mensagens, acessos a sites, redes sociais, o que eu compro, como e aonde fui, que horas desperto, qual a temperatura do lugar em que estou, o próprio lugar onde eu estou (e estava), enfim, uma imensurável quantidade de dados sobre o ser e a sua existência. Aquilo que parece ser um componente externo (aparelho) é, na essência, o maior portador da nossa interioridade. As possibilidades de invasão sobre essa esfera da vida privada são imensuráveis. O problema passa a ser o controle sobre o acesso, o controle sobre os limites da invasão. Existe (ainda) um espaço impenetrável? Ou o *ser* está desnudo? E uma vez despido da proteção, o que nos sobra? O contraditório durante os quatro momentos da prova, a oralidade e o sistema acusatório atuam de que forma efetiva? E a cadeia de custódia da prova digital, como se estabelece?
>
> Como o tamanho volume de dados e informações pessoais (e de terceiros) deveria ser protegido? O caminho previsto para sacrificar a privacidade deveria ser, no mínimo, o mesmo exigido para o ingresso em domicílio pela polícia: mandado judicial fundamentado ou diante de flagrante delito, demarcando, sobretudo, a justa causa prévia neste último caso. Sempre lembrando que o imputado jamais poderá ser compelido, nem mesmo por ordem judicial, a fornecer senhas, na medida em que protegido pelo direito de não autoincriminação. Não se pode mais continuar considerando como válido o consentimento dado pelo sujeito abordado pela autoridade policial em via pública, para que se tenha acesso ao aparelho celular (via entrega de senhas, por exemplo) e faça uma devassa incriminatória na sua vida. Sem falar que, não raras vezes, o volume de informações ali contidas acaba por virar uma verdade devassa inquisitória, uma *fishing expedition* [...][205].

Diante desse cenário, torna-se imprescindível rever – refletindo e reconsiderando – até mesmo alguns princípios do direito processual penal. Por isso, a forma de colheita das evidências – notadamente as digitais – deve ser repensada, com o fim de dar eficácia à sua prova

---

[203] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. Ed. São Paulo: Revista dos Tribunais, 2024, p. 50.
[204] LOPES Júnior, Aury. **Direito Processual Penal**. 21. edição. São Paulo: Saraivajur, 2024, p. 487.
[205] Ibid., p. 488-489.

sem, no entanto, deixar de lado todos os direitos e garantias que foram, a duras penas, conquistados.

3.4 EXPLORANDO A INTERNET: NOÇÕES FUNDAMENTAIS

A origem da internet ocorreu nos Estados Unidos, resultado de um esforço do sistema de defesa, para dotar os centros de pesquisas militares de rede de comunicações, com transferência de informações[206].

Explica Tarcísio Teixeira:

> Mais tarde, no final da década de 1980, essa tecnologia expandiu-se de forma a estabelecer a comunicação de computadores entre universidades e entre outros institutos e laboratórios de pesquisas norte-americanos, possibilitando, assim, a troca de informações mediante um sistema de protocolos – códigos que permitiam a leitura dos documentos.
> No final de abril de 1993, essa tecnologia de comunicação entre computadores já estava bem desenvolvida e, associada ao barateamento dos equipamentos, chega a ponto de favorecer sua utilização por empresas e por particulares. Nesse estágio, a comunicação é feita por meio de linha telefônica comum.
> Desse modo, foi então criada a internet, conhecida também por "rede mundial de computadores", meio pelo qual computadores do mundo são interligados, possibilitando, assim, a comunicação entre si.
> [...]
> Assim, a internet é a interligação de redes de computadores espalhadas pelo mundo, que passam a funcionar como uma só rede, possibilitando a transmissão de dados, sons e imagens de forma rápida. Essa interligação de redes pode ser feita por sistema telefônico de cabos de cobre ou de fibras óticas, por transmissão via ondas de rádio ou via satélite, por sistema de televisão a cabo etc. O usuário a ela se conecta, geralmente, por intermédio de um aparelho conhecido por *modem*, associado à utilização de programas de computadores com essa finalidade. Frise-se que, nos primeiros anos de internet massificada, o acesso era feito por computadores que, por sua vez, utilizavam modens. Atualmente, o acesso à internet é feito pelos mais variados dispositivos tecnológicos, sobretudo por *smartphones* ligando-se à rede mundial de computadores via dados móveis ou *Wi-Fi (wireless fidelity*, ou "fidelidade sem fio")[207].

É importante ir mais além acerca do surgimento da internet:

> No ano de 1957 a União Soviética lançou seu primeiro satélite espacial, o Sputnik. A contraofensiva a esse fato foi que o então presidente dos Estados Unidos John Kennedy prometeu enviar um americano para a Lua e criar um sistema de defesa à prova de destruição (O HOMEM, 2001). Com essa última finalidade, e também para acelerar o desenvolvimento tecnológico do país e coordenar atividades relacionadas com o espaço e satélites, foi criada a Agência de Investigação de Projetos Avançados (*Advanced Research Project Agency* – ARPA).
> No ano seguinte a ARPA se enfraqueceu em razão da criação da *National Aeronautics ε Space Administration* (NASA), com finalidade análoga, de um cargo no

[206] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 4
[207] Ibid., p. 4-5.

> Departamento de Defesa com atribuições semelhantes e pelo fato dos seus programas relacionados com mísseis balísticos terem sido direcionados a outros setores militares do governo.
> A saída para a ARPA foi modificar a perspectiva de pesquisa, incluindo novos projetos cujos resultados somente poderiam ser avaliados em longo prazo. Outro aspecto foi a realização de parcerias com instituições de ensino, de forma que tornou sua atuação mais técnica e científica.
> Em razão dessa mudança de foco, passaram a investir em assuntos que até então não eram adequadamente explorados, como a computação interativa e os sistemas de tempo compartilhado.
> Em 1961 a Universidade da Califórnia (UCLA) recebeu da Força Aérea o computador Q-32, da IBM, que auxiliou a inserção da informática no seio da ARPA.
> No ano seguinte (1962) a Força Aérea, com a preocupação de proteger-se de uma eventual guerra ou ataque nuclear, solicitou à empresa Rand Corporation um estudo sobre uma rede de comunicação militar descentralizada (CASTELLS, 2001, p. 14), ou seja, despida de um núcleo central, que funcionasse mesmo que fossem destruídos alguns de seus terminais. A resposta foi um relatório que recomendava que o referido órgão militar solicitasse à American Telephone & Telegraph (AT&T) a implementação do projeto. A AT&T não concordou com o projeto e, inclusive, informou que implementar o projeto que envolvia a criação de uma rede digital de pacotes seria concorrer com ela mesma, que tinha uma rede analógica baseada em comutação de circuitos [...][208].

Com o tempo, tornou-se evidente a relevância de estabelecer uma rede que conectasse computadores localizados em diferentes lugares, facilitando assim a troca de informações entre eles. Assim, criada então a ARPANET:

> No ano de 1973 realizou-se a primeira conexão internacional da ARPANET, que interligou a Inglaterra e a Noruega. No final dessa década, a ARPANET substituiu seu protocolo de comutação de pacotes, denominado *Network Control Protocol* (NPC), para *Transmition Control Protocol/Internet Protocol* (TCP/IP).
> Em 1977 realizou-se uma demonstração do protocolo TCP/IP por intermédio da utilização de três redes: a ARPANET, a RPNET e a STATNET.
> Na década de 80 a ARPANET se disseminou pelos Estados Unidos e promoveu a interligação entre universidades, órgãos militares e governo.
> Foi implementado, no ano de 1986, a NSFNET – pela *National Science Foundation* - e a ARPANET começou a ser chamada de "Internet".
> Para que ocorresse o grande salto na utilização da Internet houve estudos precursores de Ted Nelson, mas com Tim Berners-Lee e a rede WWW (*World Wide Web)* é que foram possíveis a expansão e a utilização comercial da Internet. Surgem os navegadores para facilitar a vida e utilização por usuários (LAURENTIZ, 2010).
> Assim, surge a Internet, a rede das redes, a rede mundial de computadores, tornando-se acessível a toda população mundial [...][209].

Tarcísio Teixeira também explica a estrutura:

> É a rede das redes de computadores interligados entre si, sendo que a linguagem utilizada é conhecida por "protocolo TCP-IP"; além disso, cada computador possui um endereço IP – *Internet Protocol* (número de identificação do computador). Quando se navega pela internet e se digita um nome de domínio, na verdade, está se

[208] WENDT, Emerson; Jorge, Higor Vinícius Nogueira. **Crimes Cibernéticos:** ameaças e procedimentos de investigação. 3. ed. Rio de Janeiro: Brasport, 2021, p. 5-6.
[209] Ibid., p. 7-8.

> procurando um endereço IP de um computador que abriga aquele domínio para, assim, estabelecer uma comunicação com ele. Diferentemente do sistema de telefonia convencional, em que a comunicação se dá entre duas pessoas (ou mais de duas) fechando-se um circuito para elas, em uma ligação exclusiva; na internet, a comunicação não se fecha em um circuito exclusivo, pois as mensagens são trocadas entre os usuários como se fossem pacotes que trafegam pela rede por rotas variadas.
> [...]
> Vale destacar que os provedores de acesso têm um número limitado de IP's, sendo que a cada acesso de um usuário é utilizado um IP que, ao ser desconectado, será utilizado por outro usuário, havendo uma rotatividade de IP's entre os internautas vinculados ao provedor.
> Dada a insuficiência para a expansão do número de acessos à internet, surgiu a necessidade de ampliação da sequência numeral do IP, surgindo o IPv6 (IP versão 6). O IPv6 é uma versão mais recente do IP, que, a princípio, deve conviver por um tempo com o IPv4 (IP versão 4), para posteriormente substituí-lo. A diferença fundamental entre ambos é a quantidade infinitamente maior de IP's que o IPv6 (132 *bits*) permite em relação ao IPv4 (32 *bits*).
> Quanto às rotas percorridas, diferentemente do que ocorre nas ligações telefônicas convencionais, na internet não existe apenas um caminho para a troca de dados entre dois computadores. São várias as rotas, não sendo comum, mas possível de acontecer excepcionalmente que algum pacote de dados acabe se perdendo em certa rota[210].

Dessa forma, é importante entender como a internet funciona:

> [...] consiste em uma grande rede de dados digitais composta de diversas outras redes que se interconectam e permitem a troca de dados entre cada um dos seus pontos de conexão.
> A princípio, cada um desses pontos recebe uma identificação única, através de seu endereço IP, o qual permite que a rede identifique a origem das requisições de dados e saiba para onde enviar as respostas. Só há troca de dados entre dois pontos da rede se ambos conseguirem se identificar de maneira objetiva (função desempenhada pelo sistema de endereços IP).
> [...]
> O endereço IP é uma sequência de números ou caracteres únicos para determinada conexão, que permite a troca de dados em uma rede multiconectada com diversas outras. Inicialmente havia o formato IPV4, que era uma sequência de quatro grupos de, no máximo, três números entre 1 e 255.
> Há alguns anos houve a necessidade da atualização do formato, para comportar um maior número de dispositivos. Criou-se, então, o IPV6, que adota outra sequência de letras e números [...][211].

Existem também outros elementos, a saber: (i) servidores DNS: que identificam os domínios (por exemplo: www.google.com.br); (ii) servidores de dados: computadores especializados para a função de processamentos de dados de serviços digitais (por exemplo, manter os dados de websites); (iii) servidores backbones: que integram as sub-redes, com caminhos de transferência de dados para outros locais, sendo fundamentais para a internet e acessos; (iv) provedores: que provêm o acesso à internet e, ao conectar, o usuário passa a receber um endereço IP, que o identifica na rede mundial; (v) protocolo HTTP (ou HTTPS, que

[210] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 6-7.
[211] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed. São Paulo: Revista dos Tribunais, 2024, p. 35-36.

é a versão segura): possibilita acesso a sites com uso de programas de navegação, os *browsers*, podendo haver outros, como IMAP/POP3/SMTP[212], FTP[213], SSH[214] e VPN; (vi) protocolos de comunicação: que visam padronizar o formato e os procedimentos da informação e comunicação; e (vii) processo de encriptação: com o fim de manter a privacidade e segurança do usuário utilizando, para tanto, um cálculo matemático para encobrir a informação[215].

Nesse sentido, é relevante destacar acerca do provedor (endereço IP), que:

> [...] é comum que [...] empresas usam a estratégia de IP Dinâmico, que consiste em trocar o endereço IP do usuário a cada vez que seu ponto de internet é ligado. Isso facilita o gerenciamento de seus endereços IPV4 diante de uma grande carteira de clientes.
> Apesar da mudança constante nos endereços IP de seus clientes, os provedores de conexão mantêm arquivos LOG indicando qual cliente estava usando o endereço em determinado momento, facilitando a identificação do acesso, caso necessário.
> [...]
> Por lei, os provedores de conexão no Brasil são obrigados a manter o histórico de acesso de seus clientes por até 12 meses. A identificar o endereço IP envolvido no seu caso, é possível consultar via WHOIS qual o provedor do cliente para realizar a solicitação judicial dos dados do proprietário da conexão. Porém, isso pode ficar mais difícil caso o usuário tenha usado uma VPN [...][216].

Explicitando mais tais pontos – necessários para a compreensão da prova digital como um todo – Tarcísio Teixeira destaca:

> Exemplificando e detalhando um pouco mais as espécies de provedores, vale ter em conta que *backbone*, em português, pode ser traduzido literalmente como espinha dorsal, mas em matéria de internet significa o cabeamento de altíssima velocidade capaz de interligar redes de localidades, países e continentes entre si. O provedor de *backbone* (ou de **estrutura**) gerencia grandes estruturas de rede que permitem o trânsito de dados via roteadores (dispositivos que encaminham pacotes de dados entre redes de computadores) interligados e de alta velocidade. Eles nada mais são que as operadoras de telecomunicações; havendo *backbones* **internacionais/intercontinentais**, que fazem a ligação entre continentes e/ou países, inclusive por cabos submarinos (como a GloboNet), *backbones* **nacionais** (por exemplo, a EMBRATEL) e *backbones* **estaduais/regionais** (exemplificado pela Rede

[212] "os dois primeiros são serviços para obtenção de mensagens de e-mail. Enquanto o primeiro permite receber as mensagens mantendo uma cópia nos servidores, o segundo apaga as mensagens assim que baixadas pelo usuário. Já o serviço de SMTP é focado somente no envio de mensagens de e-mail". (SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed. São Paulo: Revista dos Tribunais, 2024, p. 36).
[213] "é um serviço especializado na disponibilização de arquivos na internet. Por meio de um software especializado nesse serviço você pode realizar operações nos arquivos de um servidor". (SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed. São Paulo: Revista dos Tribunais, 2024, p. 40).
[214] "é um serviço específico para acesso à linha de comando *(shell)* de computadores remotos, permitindo realizar operações com arquivos, instalação de programas e outras operações. É muito usado para a manutenção de servidores na internet" (SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed. São Paulo: Revista dos Tribunais, 2024, p. 40).
[215] Ibid., p. 36-43.
[216] Ibid., p. 39.

> Pernambuco de Informática). Embora provedor de *backbone* não seja provedor de acesso, é possível um titular de provedor de *backbone* também ser titular de uma atividade de provedor de acesso, ou vice/versa, ficando ambas as atividades sob a "marca comercial".
> Um exemplo de prestador de serviço e fornecedor que gerencia contas de *e-mails*, ou seja, um **provedor de correio eletrônico**, é o Hotmail. Já o Locaweb exemplifica a atividade do **provedor de hospedagem** hospedando *sites*, redes sociais e *blogs*, entre outros. Ambos os provedores, de correio eletrônico e de hospedagem, utilizando-se da estrutura de provedores de *backbones*, via contrato oneroso.
> É preciso fazer uma distinção mais pormenorizada entre o **provedor de acesso** (como a NetVirtua e a Vivo/Telefônica) e o **provedor de conteúdo** (exemplificativamente, o portal Globo), os quais também se utilizam da estrutura dos *backbones*, tendo em vista que, às vezes, ambas as figuras chegam a ser confundidas.
> [...] o **Marco Civil da Internet** (Lei n. 12.965/2013), arts. 9º e seguintes, cuida do provedor de conexão e do provedor de aplicações de internet. Conforme o texto da lei, o provedor de **conexão** é uma categoria que corresponde ao provedor de acesso; já a categoria do provedor de **aplicações de internet** contempla os provedores de correio eletrônico, hospedagem e conteúdo.
> Os **provedores de acesso** [ou de conexão] surgiram na década de 1990, sendo também conhecidos por ISPs – *Internet Service Providers* (provedores de serviço de internet). Vale ressaltar que este tipo de provedor utiliza-se de um serviço de telecomunicações que lhe dá suporte, ou seja, do provedor de *backbone*.
> No Brasil, o uso de meios da rede pública de telecomunicações para acesso à internet desde 1995 estava disposto na Norma n. 004/95 [...][217].

Acerca do Virtual Private Network (VPN):

> [...] é um tipo de conexão realizada entre seu computador e um terceiro para funcionar como uma "ponte" para o acesso à internet. Ao usar o serviço, seus dados trafegam na rede local de modo protegido e o endereço IP do seu computador é omitido nas aplicações remotas. É comum seu uso em redes Wi-Fi públicas para evitar interceptação. Fornecedores desse serviço dentro do território nacional podem ser solicitados para fornecer as informações de acesso do usuário caso seja usado indevidamente[218].

Nesse ponto, denota-se que por meio de tal acesso, é possível falar-se em delitos como furto por meio de sistema eletrônico, com a consecução de acessos remotos pelo VPN a partir de endereços IPs de várias localidades, por exemplo, o que dificultaria sobremaneira a investigação criminal.

Quanto à legislação, a Norma nº 004/95 (aprovada pela Portaria nº 148/95 do Ministério das Comunicações), regulava o uso de meios da rede pública de telecomunicações para acesso à internet, definida como "conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como 'software' e os dados contidos nestes computadores" (item 3, alínea *a*) e o serviço de conexão

[217] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 11-12.
[218] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed. São Paulo: Revista dos Tribunais, 2024, p. 40.

à internet (SCI) como "nome genérico que designa Serviço de Valor Adicionado, que possibilita o acesso à Internet a Usuários e Provedores de Serviços de Informações" (item 3, alínea *d*).

No Brasil, o IBGE passou a utilizar computador UNIVAC 1105. Já no ano de 1964, houve a criação do Centro Eletrônico de Processamento de Dados do Estado do Paraná e, no ano seguinte, o Serviço Federal de Processamento de Dados, com associação junto ao consórcio internacional por satélite (International Telecommunications Satellite Organization - INTELSAT). Ainda, é criada a Empresa Brasileira de Telecomunicações. Fato é que o primeiro computador brasileiro foi criado em 1972, pela Universidade Federal de São Paulo (USP) e, posteriormente, houve a criação da Computadores Brasileiro S.A. Houve constante avanço até a possibilidade de rede comercial, em 1995[219].

Além disso, hoje, o Marco Civil da Internet (Lei nº 12.965/2014) traz diversas definições, sendo a internet o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes (artigo 5º).

Dentro desse panorama, não se pode perder de vista os agentes na internet, especialmente os usuários, que são aqueles que a utilizam efetivamente, ou seja, é internauta, independentemente de sua finalidade[220].

E, com o surgimento da era digital, o volume e a sofisticação das informações disponíveis cresceram de forma extraordinária, acarretando dificuldades consideráveis na coleta, conservação e exibição de provas em investigações e processos legais. Nesse sentido, Jones Franklin destaca:

> A tecnologia trouxe consigo novas formas de produção, armazenamento e transmissão de dados, o que torna necessário repensar os procedimentos tradicionais de cadeia de custódia. Enquanto as evidências físicas eram relativamente tangíveis e fáceis de rastrear, as evidências digitais são voláteis e podem ser facilmente modificadas ou destruídas sem deixar rastros visíveis. Isso exige a adoção de práticas e ferramentas especializadas para garantir a autenticidade, a integridade e a confiabilidade dessas evidências.
> Além disso, a velocidade da evolução tecnológica também representa um desafio. Novas tecnologias e formatos de dados surgem constantemente, o que exige que profissionais da área jurídica e peritos forenses estejam atualizados e preparados para lidar com as mudanças. A complexidade das evidências digitais requer conhecimentos específicos e especializados para extrair informações relevantes e apresentá-las de forma compreensível e convincente em um processo judicial.
> Outro aspecto importante é a questão da privacidade e proteção de dados. A tecnologia possibilitou a coleta massiva de informações pessoais, o que pode afetar a privacidade dos envolvidos em um processo. É fundamental garantir que a obtenção e o uso de

[219] WENDT, Emerson; Jorge, Higor Vinícius Nogueira. **Crimes Cibernéticos:** ameaças e procedimentos de investigação. 3. ed. Rio de Janeiro: Brasport, 2021, p. 8.
[220] TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024, p. 18.

> evidências digitais respeitem os direitos individuais e estejam em conformidade com as leis e regulamentações de proteção de dados vigentes.
> No entanto, apesar dos desafios, a tecnologia também trouxe benefícios significativos para a cadeia de custódia da prova. A utilização de métodos avançados de criptografia, por exemplo, pode assegurar a autenticidade e a integridade dos dados coletados. Além disso, o uso de ferramentas de análise forense digital pode facilitar a identificação de padrões e relações entre os dados, auxiliando na reconstrução dos eventos e no fortalecimento dos argumentos apresentados em um processo judicial.
> A agilidade na obtenção e análise de evidências digitais também é um ponto positivo. Anteriormente, a coleta de evidências físicas era um processo demorado e muitas vezes sujeito a falhas humanas. Com a tecnologia, é possível extrair rapidamente informações relevantes de grandes volumes de dados e apresentá-las de forma organizada e eficiente[221].

Dessa forma, vê-se que a tecnologia na cadeia de custódia – notadamente dentro do contexto das provas digitais – implica em constante evolução, de modo que os profissionais devem estar preparados para isso, afinal, o método pode ser considerado inadequado ou, mesmo sendo apropriado, se não houver evidências de sua utilização devido à falta de documentação da cadeia de custódia, não é possível assegurar a preservação da autenticidade e integridade dos dados digitais.

Portanto, conhecer detalhes específicos e ter capacitação técnica é essencial para sua análise, uma vez que sua natureza é delicada e suscetível a alterações.

3.5 A LEGISLAÇÃO BRASILEIRA EM PERSPECTIVA

Com efeito, não há no ordenamento qualquer denominação em relação aos meios específicos de obtenção e preservação da prova digital.

No entanto, extraem-se do CPP e de legislações especiais disposições acerca da questão. Nesse sentido, destacam-se, por exemplo: a) Lei nº 9.296/96 (Interceptações telefônicas, telemáticas e captação ambiental); b) Lei nº 8.069/90 (Estatuto da Criança e do Adolescente); e c) Lei nº 12.850/13 (Lei das Organizações Criminosas).

3.5.1 Interceptações telefônicas, telemáticas e captação ambiental (Lei 9.295/96)

O art. 1º da lei regulamentou o inciso XII do art. 5º da CF/88[222], determinando que a interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação

[221] JONES, Franklin. **Rastreando a verdade.** A cadeia de custódia da prova. Maringá: Viseu, 2023, p. 70-71.
[222] Art. 5º, XII, da CF: "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".

criminal e em instrução processual penal, dependerá de ordem do juiz competente da ação principal.

Além disso, impõe alguns requisitos para sua utilização, como não ser possível se não houver indícios razoáveis da autoria ou participação em infração penal, quando a prova puder ser realizada por outros meios disponíveis ou o fato investigado constituir infração punida com, no máximo, pena de detenção. É, portanto, meio de obtenção de prova excepcional (art. 2º).

O objetivo desse método de coleta de evidências, previsto na lei interna, é interceptar as comunicações on-line para encontrar provas de atividades criminosas.

O Pacote Anticrime inseriu o artigo 8º-A na Lei 9.296/96, de modo a sistematizar o meio de obtenção de prova denominada *captação ambiental de sinais eletromagnéticos, ópticos ou acústicos* desde que a prova não possa ser feita por outros meios disponíveis e – igualmente – eficazes e apenas quando houver elementos probatórios razoáveis de autoria e participação em infrações penais com penas máximas superiores a 4 anos (ou infrações conexas), sendo que o requerimento deve descrever circunstanciadamente o local e a forma de instalação do dispositivo de captação ambiental (art. 8º-A, § 1º).

Ora, o STJ entende ser lícita a autorização para interceptação telefônica, desde que observados os ditames normativos previstos na Lei (AgRg no RHC 183.085-SP, Rel. Min. Antonio Saldanha Palheiro, julgado em 16/4/2024 – Info 809).

Além disso, o STF entendeu pela constitucionalidade do estabelecimento, por resolução do CNMP (36/2009) de cautelas procedimentais para proteção de dados sigilosos e garantia da efetividade dos elementos de prova colhidos via interceptação telefônica, entendendo que não extrapola competência privativa da União, tampouco ofende legislação infraconstitucional (STF, Plenário, ADI 5.315/DF, Rel. Min. Roberto Barroso, julgado em 4/9/2023 – Info 1106).

No mais, constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei, com pena de reclusão de 2 a 4 anos, e multa (art. 10). Ainda, incorre na mesma pena a autoridade judicial que determina a execução de tais condutas com objetivos diversos e não autorizados em lei (art. 10, parágrafo único). Também é crime realizar captação ambiental de sinais eletromagnéticos, ópticos ou acústicos para investigação ou instrução criminal sem autorização judicial se esta for exigida, conduta que é punível com pena de reclusão, de 2 a 4 anos, e multa (art. 10-A).

Por fim, não haverá crime caso a captação seja realizada por um dos interlocutores (art. 10-A, § 1º); nesse sentido, o STJ decidiu que “a gravação ambiental em que advogados participam do ato, na presença do inquirido e dos representantes do Ministério Público,

inclusive se manifestando oralmente durante a sua realização, ainda que clandestina ou inadvertida, realizada por um dos interlocutores, não configura crime, escuta ambiental, muito menos interceptação telefônica" (5ª Turma, HC 662.960-RJ, Rel. Min. Joel Ilan Paciornik, julgado em 17/5/2022 – Info 737).

3.5.2 Estatuto da Criança e do Adolescente (Lei 8.069/90)

O Estatuto foi alterado pela Lei 13.441/2017, que introduziu o art. 190-A ao diploma, possibilitando a infiltração de agentes de polícia na internet com a finalidade de investigar crimes elencados no ECA (artigos 240 a 241-D), crimes contra a dignidade sexual, corrupção de menores, satisfação de lascívia, favorecimento de prostituição de criança, adolescente ou vulnerável e invasão de dispositivo informático.

Tal meio de obtenção de prova decorre da complexidade de investigação de tais delitos, vez que, no meio digital, podem ser utilizados subterfúgios (como pseudônimos), com o fim de dificultar a identificação. Dessa forma, na prática, o policial acessa o ambiente virtual como se fosse um usuário interessado em sites sobre pornografia infantil, por exemplo, possibilitando a identificação dos autores[223].

De todo modo, a infiltração deverá ser precedida de autorização judicial devidamente fundamentada e que estabeleça os limites da infiltração, pois é estratégia de investigação peculiar em que um policial, disfarçando sua verdadeira identidade, assume o papel de criminoso para entrar na organização criminosa. Dessa forma, busca reunir informações sobre os crimes cometidos pelo grupo, identificando seus membros, métodos de operação, locais de residência e atuação, produtos dos delitos, além de qualquer outra evidência que possa ser utilizada para desmantelar a organização e ser apresentada no processo judicial[224].

---

[223] BARROS, Guilherme Freire de Melo. **Estatuto da Criança e do Adolescente**. 14. ed. Salvador: Juspodivm, 2020, p. 278.

[224] CAVALCANTE, Márcio André Lopes. São ilegais as provas obtidas por policial militar que, designado para coletar dados nas ruas como agente de inteligência, passa a atuar, sem autorização judicial, como agente infiltrado em grupo criminoso. **Buscador Dizer o Direito**, Manaus. Disponível em https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/5fde40544cff0001484ecae2466ce96e#:~:text=por%20tempo%20limitado.-,S%C3%A3o%20ilegais%20as%20provas%20obtidas%20por%20policial%20militar%20que%2C%20designado,agente%20infiltrado%20em%20grupo%20criminoso. Acesso em: 20 de julho de 2024

3.5.3 Lei das Organizações Criminosas (Lei 12.850/13)

A infiltração virtual de agentes foi incluída também pelo Pacote Anticrime (Lei 13.964/2019) que tratou da matéria nos artigos 10-A a 10-D.

Aqui, será possível a ação de agentes de polícia infiltrados virtualmente para investigar não apenas os crimes previstos na Lei de Organização Criminosa, mas também aqueles conexos. Contudo, somente poderá ocorrer se for demonstrada sua necessidade, além de indicados o alcance das tarefas dos policiais e das pessoas investigadas, bem como dados de conexão para identificação de todos.

Além disso, na lei consta a necessidade de serem definidos os dados de conexão e de cadastros, sendo aquelas:

> [...] informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão, ao passo que estas são informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão (art. 10-A).

A infiltração será autorizada pelo prazo de até 6 meses, sendo possível renovações, desde que haja ordem judicial fundamentada e não exceda a 720 dias (art. 1º-A, § 4º).

Interessante destacar que não cometerá crime o policial que oculta sua identidade para, por meio da internet, colher indícios de autoria e materialidade (art. 10-C).

A autorização para a infiltração digital é essencial na investigação de delitos cibernéticos, especialmente os cometidos por meio da *deep web* e *dark web*, considerando os desafios envolvidos na apuração desses crimes. É crucial lembrar que essa infiltração só é possível em situações em que há a prática de crimes por uma organização criminosa ou em crimes relacionados, o que limita sua aplicação em diversos casos significativos. Esse aspecto deveria ter sido levado em conta pelo legislador, de modo a possibilitar a infiltração virtual em situações de grande gravidade. Assim, estaria assegurado o critério da necessidade rigorosa de suspensão das garantias constitucionais, em conformidade com o princípio da proporcionalidade[225].

Recentemente, o STJ decidiu ser possível a utilização de ações encobertas, controladas virtuais ou de agentes infiltrados no plano cibernético, inclusive por meio de espelhamento do Whatsapp Web, desde que amparada por autorização judicial. Nesse sentido:

---

[225] MOURA, Grégore Moreira de. **Curso de Direito Penal Informático**. Belo Horizonte, São Paulo: D'Plácido, 2021, p. 292.

> A potencialidade danosa dos delitos praticados por organizações criminosas, pelo meio virtual, aliada a complexidade e dificuldade da persecução penal no âmbito cibernético devem levar a jurisprudência a admitir as ações controladas e infiltradas no mesmo plano virtual. De fato, nos últimos anos, as redes sociais e respectivos aplicativos se tornaram uma ferramenta indispensável para a comunicação, interação e compartilhamento de informações em todo o mundo. Entretanto, essa rápida expansão e influência também trouxeram consigo uma série de desafios e problemas no âmbito da investigação, no meio virtual, tornando-se a evolução da jurisprudência acerca do tema questão cada vez mais relevante e urgente.
> Impositivo se mostra o estabelecimento de regras processuais compatíveis com a modernidade do crime organizado, porém, sempre respeitando, dentro de tal quadro, os direitos e garantias fundamentais do investigado. Tal desiderato restou alcançado na medida em que, no ordenamento pátrio, a infiltração, igualmente a outros institutos que restringem garantias e direitos fundamentais, está submetida ao controle e amparada por ordem de um juiz competente.
> Não há empecilho, portanto, na utilização de ações encobertas ou agentes infiltrados na persecução de delitos, pela via dos meios virtuais, desde que, conjugados critérios de proporcionalidade (utilidade, necessidade), reste observada a subsidiariedade, não podendo a prova ser produzida por outros meios disponíveis.
> É o que se dá na hipótese em análise, com o autorizado espelhamento via *Whatsapp Web*, como meio de infiltração investigativa, na medida em que a interceptação de dados direta, feita no próprio aplicativo original do *Whatsapp*, se denota, por vezes, despicienda, em face da conhecida criptografia ponta a ponta que vigora no aplicativo original, impossibilitando o acesso ao teor das conversas ali entabuladas. Concebe-se plausível, portanto, que o espelhamento autorizado via *Whatsapp Web*, pelos órgãos de persecução, se denote equivalente à modalidade de infiltração do agente, que consiste em meio extraordinário, mas válido, de obtenção de prova.
> Pode, desta forma, o agente policial valer-se da utilização do espelhamento pela via do *Whatsapp Web*, desde que respeitados os parâmetros de proporcionalidade, subsidiariedade, controle judicial e legalidade, calcado pelo competente mandado judicial [...][226].

Portanto, as ações controladas que englobam a utilização de agentes infiltrados digitais são permitidas no ordenamento, sendo medida que garante a legitimidade do monitoramento das comunicações, como fundamental para prevenção e repressão ao crime.

3.6 MEIOS DE OBTENÇÃO E A CADEIA DE CUSTÓDIA SOB O ENFOQUE DA PROVA DIGITAL

Diante da importância de manter a integridade da prova, o legislador, em 2019, com o Pacote Anticrime, dedicou novo capítulo ao Código de Processo Penal, tratando da "cadeia de custódia", no artigo 158-A do CPP, como sendo "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou

[226] BRASIL. Superior Tribunal de Justiça. **AgRg no AREsp nº 2.218.334**/MG, Rel. Min. Reynaldo Soares da Fonseca, Quinta Turma, julgado em 16/4/2024, DJe 23/4/2024.

em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".

Acerca do tema, Renato Brasileiro discorre:

> [...] se destaca a importância do estudo da chamada *cadeia de custódia*, que consiste, em termos gerais, em um mecanismo garantidor da autenticidade das evidências coletadas e examinadas, assegurando que correspondem ao caso investigado, sem que haja lugar para qualquer tipo de adulteração. Funciona, pois, como a documentação formal de um procedimento destinado a manter e documentar a história cronológica de uma evidência, evitando-se, assim, eventuais interferências internas e externas capazes de colocar em dúvida o resultado da atividade probatória, assegurando, assim, o rastreamento da evidência desde o local do crime até o Tribunal [...]
> A preocupação com o tema não é nova. Ganhou destaque, na verdade, em meados da década de 90, nos Estados Unidos da América, quando o ex-jogador de futebol americano e então ator O. J. Simpson, acusado de ser o executor do homicídio de sua ex-esposa e de um amigo dela, foi absolvido. Como destaca Michelle Moreira Machado, "mesmo diante de provas que demonstravam o envolvimento do jogador em um duplo homicídio, a defesa conseguiu a absolvição devido à preservação do local inadequada, aos procedimentos de coleta de vestígios incorretos em que ficaram evidentes falhas na cadeia de custódia".
> Em um sistema processual penal regido pela presunção de inocência e pelo devido processo legal, e inspirado em uma matriz processual consentânea com o modelo acusatório, estrutura básica para a realização de um processo equitativo, há de se tutelar com muito cuidado a atividade probatória, assegurando-se à defesa não apenas o conhecimento da acusação, mas também à ciência dos meios e fontes de prova existentes [...]
> Aplicável a todo e qualquer elemento probatório (v.g., drogas, *res furtiva*, mídia digitais, etc.), a cadeia de custódia tem início com a preservação do local do crime ou com procedimentos policiais ou periciais nos quais seja detectada a existência de vestígios, e se encerra tão somente com o descarte do vestígio, geralmente ao final do processo penal[227].

É, portanto, mecanismo – essencial - para garantir a autenticidade das provas coletadas e analisadas, certificando-se de que estão em conformidade com o ordenamento jurídico e com o caso concreto, afastada, portanto, a possibilidade de manipulação.

Segundo Geraldo Prado:

> Um dos aspectos mais delicados na temática da aquisição de fontes de prova consiste em preservar a idoneidade de todo o trabalho que tende a ser realizado sigilosamente, em um ambiente de reserva que, se não for respeitado, compromete o conjunto de informações que eventualmente venham a ser obtidas dessa forma. Trata-se de evitar o fenômeno da <<break on the chain of custody>>.
> [...]
> Os suportes técnicos que resultam da operação, portanto, devem ser preservados. A razão adicional, de natureza constitucional, está vinculada ao fato de que apenas dessa maneira é possível assegurar à defesa, oportunamente, o conhecimento das fontes de prova.
> O rastreamento das fontes de prova será uma tarefa impossível se parcela dos elementos probatórios colhidos de forma encadeada vier a ser destruída. Sem esse

[227] LIMA, Renato Brasileiro. **Pacote Anticrime.** Comentários à Lei 13.964/19. Salvador: JusPodivm, 2020, p. 251-252.

> rastreamento, a identificação do vínculo eventualmente existente entre uma prova aparentemente lícita e outra, anterior, ilícita, de que a primeira é derivada, dificilmente será relevado.
> Os suportes técnicos, pois, têm uma importância para o processo penal que transcende a simples condição de ferramentas de apoio à polícia para a execução de ordens judiciais.
> [...]
> A preservação destes elementos probatórios, portanto, insere-se no âmbito de juridicidade que, observada a inexistência de previsão legal, deve ser suprido pelo juiz para garantir ao processo a sua qualidade de entidade epistêmica[228].

A análise dos delitos digitais continua a apresentar importantes obstáculos para as polícias judiciárias no Brasil, que precisam progredir na implementação de novas técnicas para identificar os responsáveis e comprovar a existência do crime[229].

É, portanto, modo de registrar um procedimento, com o objetivo de preservar e documentar a linha do tempo de uma evidência, prevenindo possíveis interferências internas e externas que possam questionar o resultado da investigação, garantindo assim a rastreabilidade da prova desde o local do crime até o julgamento do caso. Para além disso, visa a proteção dos direitos das partes envolvidas, desde a investigação, até o procedimento judicial.

Por conseguinte, é essencial que todas as fases sejam documentadas de maneira minuciosa, assegurando um processo equitativo e que respeite os direitos fundamentais. Dessa forma, a gestão da cadeia de custódia das provas exerce um impacto significativo na convicção dos juízes, já que a correta preservação das evidências é crucial para que o magistrado consiga analisar adequadamente os elementos probatórios e emitir uma decisão embasada, garantindo, dessa maneira, a imparcialidade e a justiça do julgamento.

Os dispositivos físicos envolvidos em crimes cibernéticos (como computadores, tablets, smartphones, entre outros) deverão obedecer a toda a cadeia de custódia, garantindo a preservação adequada das evidências relacionadas a esses delitos, com a proteção dos dados obtidos de tais equipamentos, de forma a evitar qualquer tipo de alteração ou comprometimento[230].

Aliás, a cadeia de custódia guarda direta correlação com a busca da verdade processual, outrora objeto de estudo. Nesse sentido:

> [...] É um procedimento que envolve a documentação e o controle cuidadoso de todas as evidências físicas e materiais relevantes para um caso, desde o momento da coleta

---

[228] PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos** – A quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014, p. 77-79.
[229] BARRETO, Alesandro Gonçalves; SANTOS, Hericson dos. **Deep Web:** Investigação no submundo da internet. Rio de Janeiro: Brasport, 2019, p. 83.
[230] MOURA, Grégore Moreira de. **Curso de Direito Penal Informático**. Belo Horizonte, São Paulo: D'Plácido, 2021, p. 308.

> até sua apresentação em tribunal. A importância dessa cadeia reside em vários aspectos.
> Em primeiro lugar, a cadeia de custódia garante a integridade e autenticidade das evidências. Ao rastrear minuciosamente o histórico de posse, desde o momento em que uma prova é obtida até o momento em que é apresentada em tribunal, é possível garantir que ela não tenha sido adulterada, substituída ou corrompida de alguma forma. Isso é essencial para acreditar na sua validade e confiabilidade.
> Em segundo lugar, a cadeia de custódia garante a transparência do processo legal. Ao registrar todas as pessoas que tiveram acesso às evidências e os momentos em que isso ocorreu, cria-se um registro claro e transparente, que pode ser verificado e auditado por todas as partes envolvidas. Isso ajuda a evitar alegações de manipulação ou violação das provas, promovendo a confiança no sistema judicial.
> Além disso, a cadeia de custódia protege os direitos dos acusados. Ao documentar cada etapa da custódia das evidências, incluindo sua embalagem, transporte, armazenamento e análise, garante-se que os procedimentos tenham sido realizados de acordo com os requisitos legais e padrões estabelecidos. Isso ajuda a evitar a violação dos direitos dos acusados e a garantir que a coleta de evidências tenha sido realizada de maneira justa e imparcial.
> Outro ponto importante é que a cadeia de custódia permite uma investigação mais precisa e eficaz. Ao manter um registro detalhado de todas as evidências e das pessoas responsáveis por elas, facilita-se a identificação e o rastreamento das fontes de prova. Isso auxiliar os investigadores e promotores na reconstrução dos eventos e na conexão entre os elementos que compõem o caso, contribuindo para a busca da verdade processual.
> Por fim, a cadeia de custódia desempenha um papel crucial na preservação das evidências ao longo do tempo. Ao garantir que as provas sejam armazenadas adequadamente e protegidas contra danos, perda ou contaminação, preserva-se sua integridade e potencial probatório. Isso permite que as partes envolvidas no processo tenham acesso a evidências confiáveis mesmo após um longo período de tempo, garantindo a justiça e a imparcialidade do sistema[231].

O artigo 158-B do CPP descreve de maneira didática a cadeia de custódia, com todas as suas etapas: (i) "*reconhecimento*: ato de distinguir um elemento como de potencial interesse para a produção da prova pericial"; (ii) *isolamento*: ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime"; (iii) "*fixação*: descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento"; (iv) "*coleta*: ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza"; (v) "*acondicionamento*: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento"; (vi) "*transporte*: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperaturas, entre outras), de modo

[231] JONES, Franklin. **Rastreando a verdade.** A cadeia de custódia da prova. Maringá: Viseu, 2023, p. 23-25.

a garantir a manutenção de suas características originais, bem como o controle de sua posse"; (vii) "*recebimento*: ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu"; (viii) "*processamento*: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito"; (ix) "*armazenamento*: procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado, com vinculação ao número do laudo correspondente"; e (x) "*descarte*: procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial".

O que se vê, é, acima de tudo, a necessidade de um sistema concatenado que confira segurança em todo o rastreamento.

Conforme a lição de Gustavo Badaró, é:

> [...] um procedimento de documentação ininterrupta, desde o encontro da fonte de prova, até a sua juntada no processo, certificando onde, como e sob a custódia de pessoas e órgãos foram mantidos tais traços, vestígios ou coisas, que interessam à reconstrução histórica dos fatos no processo, com a finalidade de garantir sua identidade, integridade e autenticidade[232].

Segundo Renato Brasileiro:

> [...] funciona, pois, como a documentação formal de um procedimento destinado a manter e documentar a história cronológica de uma evidência, evitando-se, assim, eventuais interferências internas ou externas capazes de colocar em dúvida o resultado da atividade probatória, assegurando, assim, o rastreamento da evidência desde o local do crime até o Tribunal. Fundamenta-se no chamado **princípio da 'autenticidade da prova' (ou princípio da mesmidade)**, um princípio básico pelo qual se entende que determinado vestígio relacionado à infração penal, encontrado, por exemplo, no local do crime, é o mesmo que o magistrado está usando para formar seu convencimento. Daí o porquê de tamanho cuidado na formação e preservação dos elementos probatórios no âmbito processual penal[233].

---

[232] BADARÓ, Gustavo. A cadeia de custódia e sua relevância para a prova penal. *In:* SIDI, Ricardo; LOPES, Anderson B. (org.). **Temas atuais da investigação preliminar no processo penal**. Belo Horizonte: D'Plácido, 2018, p. 523.

[233] LIMA, Renato Brasileiro. **Manual de Processo Penal** – volume único. São Paulo: Juspodivm, 2022, p. 623.

Todo esse cuidado não poderia ser diferente. Afinal, se ao analisar, por exemplo, o procedimento realizado em um simples laboratório durante uma coleta de sangue, nota-se uma série de medidas adotadas pelo profissional responsável – como a higienização das mãos, uso de luvas descartáveis, apresentação de seringas e agulhas lacradas, com toda identificação do material coletado – não poderia ser de outro modo a coleta e preservação das provas dentro do processo, com todas as precauções com o intuito de prevenir possíveis erros no resultado de um processo no contexto criminal[234]. Nesse sentido:

> É dizer, se imaginarmos que alguém foi flagrado vendendo determinado entorpecente, incumbe às autoridades responsáveis pela persecução penal comprovar que, desde o momento inicial em que a droga veio para a custódia dos órgãos persecutórios, não houve a perda da evidência, nenhum tipo de adulteração, nem tampouco qualquer forma de contaminação, seja por outros elementos, seja pelo próprio recipiente no qual a substância foi armazenada. Daí porque a droga é embalada, etiquetada e lacrada, documentando-se todos os procedimentos dessa custódia ao longo da persecução penal[235].

No contexto das provas digitais, sua importância é evidenciada, notadamente diante da facilidade quanto à manipulação, o que, em consequência, demanda cautela para que sejam mantidas de forma íntegra, autêntica e protegida, requisitos essenciais para sua aceitação e uso no processo penal. Evitar a modificação de informações, a falsificação de gravações de voz e a corrupção de arquivos de áudio, por exemplo, é o principal objetivo da cadeia de custódia acerca da evidência eletrônica.

Nesse sentido, Alexandre Morais da Rosa:

> [...] nos casos de interceptação telefônica, de dados, agente infiltrado, captação ambiental, imagens, filmagens, dentre outras modalidades ocultas, a manutenção de todo o material obtido, com a exclusão por parte do julgador e não do jogador unilateralmente, capaz de gerar a incidência do contraditório efetivo, é condição à validade da prova. A juntada parcial, deletada, omitida, de boa-fé ou má-fé, traz consigo a ilicitude da prova e a contaminação das provas dela decorrentes[236].

Desta forma, é fundamental ter cautela no manuseio das evidências digitais coletadas durante uma investigação policial e sua posterior introdução no processo judicial, especialmente no que diz respeito à cadeia de custódia. É necessário seguir um protocolo adequado de armazenamento e descarte das provas, levando em consideração as particularidades das provas digitais.

---

[234] LIMA, Renato Brasileiro. **Manual de Processo Penal** – volume único. São Paulo: Juspodivm, 2022, P. 623.
[235] LIMA, loc. cit.
[236] ROSA, Alexandre Morais da. **Guia compacto do processo penal conforme a teoria dos jogos**. 3. ed. Florianópolis: Empório do Direito, 2016, p. 242.

Fato é que o art. 158-B do CPP, como se viu, estabeleceu as etapas na cadeia de custódia, havendo o *reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento* e *descarte*.

Em consequência, vê-se a necessidade também da atuação de profissionais capacitados para tanto, com conhecimentos acerca das técnicas adequadas com o fim de garantir a integridade daquela prova, notadamente a informática forense.

Esses especialistas exercem papéis fundamentais na obtenção, conservação e avaliação de provas, assegurando a fidelidade e a segurança dos componentes que formam a evidência em um caso penal e, segundo Franklin Jones:

> Considerando a importância da cadeia de custódia no sistema de justiça, uma vez que garante a integridade e a confiabilidade das provas utilizadas nos processos legais, o treinamento e a qualificação dos profissionais envolvidos nessa cadeia são aspectos essenciais para o bom funcionamento do sistema.
> O treinamento adequado dos profissionais envolvidos na cadeia de custódia é necessário para garantir a correta manipulação e preservação das evidências. Aprender técnicas de coleta, embalagem, transporte e armazenamento seguro dos materiais é crucial para evitar contaminações, deteriorações ou perdas, o que poderia comprometer a sua validade e confiabilidade em um processo judicial
> Além disso, a qualificação dos profissionais também abrange o conhecimento das leis e normas que regem a cadeia de custódia. É importante que os envolvidos estejam atualizados com as legislações pertinentes e sigam os protocolos estabelecidos para garantir a admissibilidade das provas, bem como a proteção dos direitos dos envolvidos.
> [...]
> Outro aspecto relevante é a capacidade de lidar com situações adversas e imprevistas que possam surgir durante a cadeia de custódia. Os profissionais devem ser treinados para tomar decisões rápidas e eficientes, assegurando a continuidade e a integridade do processo, mesmo diante de desafios complexos ou pressões externas.
> Além disso, o treinamento contínuo é essencial para acompanhar o avanço tecnológico e científico na área forense. Novos métodos de análise e técnicas surgem constantemente, e é fundamental que os profissionais estejam atualizados e capacitados para utilizar essas ferramentas de maneira adequada, garantindo a precisão e a confiabilidade dos resultados.
> Em suma, o treinamento e a qualificação dos profissionais envolvidos na cadeia de custódia são cruciais para a manutenção da integridade do sistema de justiça Através de uma formação sólida e contínua, é possível assegurar que as provas sejam coletadas, preservadas e analisadas de forma segura e confiável. Dessa forma, garantimos a justiça e o respeito aos direitos de todos os envolvidos no processo legal[237].

Transportando tais ideias para as evidências digitais, tem-se a necessidade de debate e concentração em estabelecer novos horizontes, sempre balizado pelos direitos já constitucionalmente consolidados, uma vez que visa a preservação da prova, para constituição de elemento à fiabilidade da prova penal. É dizer que de nada adianta evitar, a todo custo, visar

[237] JONES, Franklin. **Rastreando a verdade.** A cadeia de custódia da prova. Maringá: Viseu, 2023**,** p. 40-43.

a preservação da prova se, ao mesmo tempo, ferir preceitos principiológicos próprios do processo penal.

É fato que em um smartphone, por exemplo, não se concentram apenas informações profissionais. Dessa forma, a simples perícia em um aparelho que poderia, num primeiro momento, revelar-se como necessária e fundamental para a persecução penal, pode culminar em violação da intimidade o que, mais adiante, poderia conduzir, num segundo ponto, à própria nulidade daquela evidência. Assim, a finalidade da persecução penal deve se concentrar especialmente em manter íntegra e utilizável aquela prova, sob pena de se perder todos os esforços concentrados em sua obtenção.

Como destaca Jones Franklin, ao mesmo tempo que a tecnologia se mostra muito importante dentro da própria cadeia de custódia, também apresenta desafios legais. Isso porque:

> A rápida evolução tecnológica requer que os sistemas e as ferramentas utilizadas na coleta e análise de evidências estejam em conformidade com as leis e regulamentos aplicáveis. Além disso, é necessário garantir que os profissionais envolvidos estejam devidamente treinados e atualizados para lidar com as complexidades das evidências digitais.
> As questões éticas e legais relacionadas à cadeia de custódia da prova exigem uma abordagem cuidadosa e atenta. É essencial garantir a integridade das evidências, respeitar a privacidade dos envolvidos, cumprir as leis aplicáveis e adotar práticas transparentes e documentadas. A garantia de uma cadeia de custódia adequada é fundamental para assegurar a justiça e a confiabilidade do processo judicial[238].

A cadeia de custódia digital possui os mesmos elementos da prevista no art. 158-A do CPP, sempre observando a importância de resguardar a integridade e a autenticidade da prova, afinal, a tecnologia está se tornando cada vez mais essencial para aprimorar esse procedimento. A implementação de sistemas computacionais e repositórios de dados digitais simplifica a documentação e a recuperação de informações, elevando a eficiência e a confiabilidade da cadeia de custódia. Essas ferramentas também possibilitam a conservação de registros eletrônicos, que ganham maior relevância em investigações relacionadas a evidências digitais. Nesse contexto, é fundamental anotar detalhes importantes, como a data, o local e as circunstâncias em que foram coletadas, pois a falta de um controle apropriado sobre as evidências pode dar margem a questionamentos sobre a violação de direitos fundamentais.

Daí porque a necessidade de que as ações “sejam claramente documentadas e registradas. Isso inclui a identificação dos responsáveis pela manipulação das evidências, as

[238] JONES, Franklin. **Rastreando a verdade.** A cadeia de custódia da prova. Maringá: Viseu, 2023, p. 75.

datas e horários em que as ações ocorreram, bem como a descrição detalhada de cada procedimento realizado"[239].

A preocupação com os procedimentos em relação à prova pericial foi exteriorizada na exposição de motivos do PL 10.372/2018 (Lei 13.964/2019), nos seguintes termos:

> A disciplina da cadeia de custódia para maior eficiência da perícia criminal e consequente combate à criminalidade também é essencial. A cadeia de custódia é fundamental para garantia e idoneidade e a rastreabilidade dos vestígios, com vistas a preservar a confiabilidade e a transparência da produção da prova pericial até a conclusão do processo judicial. A garantia da cadeia de custódia confere aos vestígios certificação de origem e destinação e, consequentemente, atribui à prova pericial resultante de sua análise, credibilidade e robustez suficientes para propiciar sua admissão e permanência no elenco probatório. Com a criação de centrais de custódia, é possível garantir que os materiais relacionados a crimes estarão sempre à disposição da polícia e da Justiça quando for necessária a realização de novas perícias a fim de dirimir dúvidas que surjam no decorrer do inquérito policial ou processo criminal[240].

Segundo Geraldo Prado:

> A indispensabilidade de um eficiente sistema de controles epistêmicos goza de especial importância nos dias atuais, porque vulgarizou-se o apelo, no âmbito da investigação, aos métodos ocultos de pesquisa (interceptação das comunicações e afastamento de sigilos) e de um modo geral a totalidade dos elementos informativos que subsidiam acusações encontra-se alicerçada em elementos obtidos dessa maneira[241].

Diante do contexto social, econômico e jurídico em que se deu a mudança na legislação do Pacote Anticrime, é fundamental ressaltar que o objetivo da lei passou de combater a impunidade para regulamentar a atividade de investigação, visando torná-la mais justa e transparente, entre outras questões, na obtenção de provas.

Fato é que a cadeia de custódia não está normatizada de forma robusta, notadamente no que tange à prova digital, daí porque cabe, num primeiro momento, à doutrina e à jurisprudência a análise e regulação do assunto.

A despeito da aparência de insegurança jurídica, não se pode olvidar que isso deve ocorrer. A possibilidade de interpretação não se dá apenas para suprir lacunas, mas sim pela própria alterabilidade de toda evidência digital, afinal, a cada dia, novas tecnologias surgem, o que seria impossível ao legislador prever todas as possibilidades.

---

[239] JONES, Franklin. **Rastreando a verdade.** A cadeia de custódia da prova. Maringá: Viseu, 2023, p. 44-45.
[240] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 10.372**, de 06 de junho de 2018. Introduz modificações na legislação penal e processual penal para aperfeiçoar o combate ao crime organizado [...]. Brasília, 2018. Disponível em:https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1666497&filename=PL%201037 2/2018. Acesso em: 05 ago. 2023.
[241] PRADO, Geraldo. **A cadeia de custódia da prova no processo penal.** São Paulo: Marcial Pons, 2019, p. 68.

Dessa forma, ainda que haja a criação de norma específica – processo penal digital – sempre haverá, ao final, a necessidade de interpretação de modo a conferenciar diálogo entre os dispositivos legais e conceitos principiológicos, de modo a evitar qualquer retrocesso.

A recolha da prova digital – notadamente dados em nuvem – deve, inicialmente, entender o objeto sobre o qual recai. Nesse sentido, entender como ocorre a conexão e todas as suas peculiaridades é imprescindível para que seja mantida sua integridade.

Nesse sentido, a própria confidencialidade e o controle de acesso são fundamentais, em um sistema de arquivamento de modo devidamente estruturado:

> [...] é necessário estabelecer um controle rigoroso de acesso às evidências. Isso implica em restringir a entrada apenas a pessoas autorizadas e devidamente treinadas, como agentes de segurança, peritos e profissionais do sistema de justiça. O acesso deve ser registrado, preferencialmente por meio de um sistema de identificação, para possibilitar a rastreabilidade e identificar possíveis irregularidades.
> [...]
> Outro aspecto relevante é a preservação do sigilo das evidências. O acesso a informações sensíveis deve ser restrito e apenas pessoas com autorização prévia devem ter conhecimento desses detalhes. É importante também evitar a exposição das evidências a pessoas não autorizadas, garantindo que apenas profissionais qualificados tenham acesso a elas.
> Além do controle de acesso, é essencial manter registros precisos sobre a movimentação das evidências. Cada etapa do processo, desde a obtenção até o armazenamento e apresentação em juízo, deve ser devidamente documentada, registrando datas, horários, responsáveis e detalhes relevantes. Esses registros ajudam a garantir a transparência e a rastreabilidade das evidências, permitindo que qualquer irregularidade seja identificada e investigada.
> É fundamental que as instalações de armazenamento das evidências sejam regularmente inspecionadas e auditadas. Essas inspeções devem ser realizadas por profissionais especializados, a fim de verificar a conformidade com os protocolos de segurança estabelecidos e garantir a adoção das melhores práticas na cadeia de custódia. Caso sejam identificadas falhas ou vulnerabilidades, é necessário adotar medida corretivas imediatas.
> O controle de acesso e a segurança das evidências na cadeia de custódia da prova são aspectos cruciais para assegurar a confiabilidade e a imparcialidade do processo judicial. A restrição de acesso, a implementação de medidas de segurança física, a preservação do sigilo, o registro detalhado das movimentações e a realização de inspeções regulares são estratégias que contribuem para a proteção das evidências e para a garantia de um sistema de justiça confiável e justo[242].

É importante manter um registro – detalhado – das etapas do processo, visando a manutenção da transparência e a rastreabilidade das provas[243], notadamente quando se trata de evidências digitais, já que suas características intrínsecas fazem com que suas alterações não sejam visíveis a olho nu.

---

[242] JONES, Franklin. **Rastreando a verdade.** A cadeia de custódia da prova. Maringá: Viseu, 2023, p. 55-57.
[243] Ibid., p. 64.

Dessa forma, não se pode olvidar da necessidade de registro de todas as transferências e remessa:

> O registro adequado das transferências e remessas das provas é essencial para assegurar a admissibilidade das evidências em um processo legal. O cumprimento rigoroso desses registros fortalece a confiabilidade e a credibilidade das provas apresentadas, uma vez que evidencia sua origem e os responsáveis por sua guarda e transporte.
> Além disso, o registro das transferências e remessas das provas na cadeia de custódia garante a transparência e a rastreabilidade do percurso das evidências. Cada vez que uma prova é transferida ou remetida, é necessário registrar detalhadamente os dados relevantes, como a data, a hora, o local e as pessoas envolvidas no processo. Isso permite que qualquer alteração ou irregularidade seja identificada e investigada, preservando a integridade das provas.
> [...]
> Adicionalmente, o registro das transferências e remessas das provas na cadeia de custódia facilita a colaboração entre os profissionais envolvidos no processo legal. Ao documentar de maneira clara e precisa todas as movimentações das evidências, promove-se a comunicação e o compartilhamento de informações entre os diversos atores, como investigadores, peritos e advogados, garantindo uma condução adequada e suficiente do caso.
> Em síntese, o registro das transferências e remessas das provas na cadeia de custódia desempenha um papel crucial na preservação da integridade e autenticidade das evidências em processos legais. Por meio desse registro, assegura-se a admissibilidade das provas, promove-se a transparência e a rastreabilidade, protege-se contra perdas e manipulações indevidas, além de facilitar a colaboração entre os profissionais envolvidos. Portanto, é imprescindível que sejam implementados procedimentos adequados e rigorosos de registro, visando garantir a justiça e a imparcialidade nos sistemas legais[244].

A preservação do conteúdo deve ocorrer já na investigação policial, aplicando-se, para as provas digitais, o disposto no art. 6º do CPP que determina que a autoridade policial, logo que tiver conhecimento da prática da infração penal, deverá "dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas".

Ora, da mesma forma, toda a evidência digital – notadamente diante de suas características – deve ser devidamente preservada. Assim:

> À vista disso, quando um homicídio é praticado, a preservação do local do crime é deveras importante e, caso não seja feita a contento, diversas evidências podem ser destruídas, comprometendo, sobremaneira, a individualização da autoria e a materialidade delitiva.
> Da mesma forma, o disposto no CPP deve ser aplicado nos crimes informáticos. Ou seja, o investigador deve ter em mente os passos necessários para preservação do crime em meio cibernético. A evidência produzida nesse meio virtual caracteriza-se pela volatilidade, devendo oportunamente ser salvaguardada, sob pena de prejudicar consideravelmente a investigação policial em andamento. Essa ação, todavia, não

[244] JONES, Franklin. **Rastreando a verdade.** A cadeia de custódia da prova. Maringá: Viseu, 2023, p. 66-68.

> deve ser confundida e em nenhum momento substituirá os exames periciais a serem realizados posteriormente[245].

Aliás, vê-se que a cadeia de custódia é sequência de atos cronológicos e sua quebra pode significar ilicitudes, ou seja, "os vestígios colhidos em desacordo com a cadeia de custódia são nulos, devendo ser desentranhadas da investigação ou do processo"[246].

Dentro desse contexto, é fundamental discutir a implementação de normas específicas para os dados que serão coletados.

Conforme se verifica cotidianamente em sites e redes sociais, ao efetuar uma pesquisa, o algoritmo retém os dados pessoais. Portanto, navegar na internet é o equivalente a deixar rastros, como o DNA em um local físico (com a diferença de que não se trata de evidência biológica).

A ideia é a seguinte: caso ocorra a prática de um delito por meio virtual, será viável examiná-lo e, consequentemente, conduzir as devidas investigações.

Ora, é evidente que todo criminoso – esteja no âmbito virtual ou não, deixará algum possível rastro, que indica sua ação. Como destaca Grégore Moreira:

> Na modernidade líquida, ser cidadão significa ter inclusão digital, mas, para isso, paga um preço que é a disponibilização de diversos dados pessoais.
> Para acessar ou participar efetivamente de aplicativos ou ter acesso a vários serviços na internet, o usuário precisa disponibilizar diversos dados como nome, *e-mail*, endereço, data de nascimento, número do cartão de crédito, além de outros dados não obrigatórios como raça, etnia, preferências religiosas e políticas.
> Malgrados esses dados possam ser falsos, já que criminosos podem inclusive usar dados de terceiros, a sua análise sempre é um bom ponto de partida para a investigação criminal.
> Acoplado aos dados cadastrais podem vir outras informações como itinerário, lugares visitados, deslocamentos realizados, transporte utilizado, entre outros.
> O uso de aplicativos como Waze, Google Maps, Uber deixam rastros, o que traz elementos importantes para a investigação criminal, mormente, para análise de álibis e entendimento do *iter criminis*[247].

É possível, a título de exemplo, considerar a seguinte situação: por meio de investigações on-line, a polícia descobre material contendo pornografia infantil no IP1. Imediatamente, esse conteúdo é removido. No entanto, essa ação não é suficiente, pois geralmente existe uma grande rede por trás disso, formando uma organização criminosa com o objetivo de cometer tais crimes. Nesse sentido, será necessário obter informações sobre o IP1.

---

[245] BARRETO, Alesandro Gonçalves; SANTOS, Hericson dos. **Deep Web:** Investigação no submundo da internet. Rio de Janeiro: Brasport, 2019.
[246] MOURA, Grégore Moreira de. **Curso de Direito Penal Informático**. Belo Horizonte, São Paulo: D'Plácido, 2021, p. 309.
[247] Ibid., p. 380.

Com o passar do tempo, descobre-se que o IP2 também possui material suspeito e, ao analisar a forma como operam, nota-se uma possível conexão com o primeiro IP identificado. A partir disso, novas investigações serão iniciadas e, com evidências mais sólidas, poderá ser solicitada uma autorização judicial para proceder com a investigação[248].

Contudo, é importante ressaltar que não se busca a divulgação ou acesso irrestrito aos dados. Pelo contrário, o foco está em uma investigação mais detalhada e precisa.

A evidência eletrônica é ferramenta de grande relevância no contexto do direito processual brasileiro, notadamente se analisada a metarrealidade. Assim:

> [...] é impossível transportar a realidade fática *in totum* para o processo penal, o que gera uma relativização no conceito de verdade real, ainda que a mesma deva ser buscada nos autos.
> Portanto, quanto mais houver verificabilidade, maior a aproximação com a realidade fática, bem como com a verdade real.
> Na cadeia de custódia não é diferente. As regras devem ser observadas, a fim de garantir a maior verificabilidade [...]
> O que se propõe com o sistema garantista, é diminuir estas incertezas, com o aumento das garantias penais e processuais, tornando o processo mais justo, pois estará mais próximo da verdade, sendo que o mesmo deve ser considerado na cadeia de custódia. [...]
> Cadeia de custódia respeitada e íntegra é parte essencial do devido processo legal, do contraditório e da ampla defesa, o que reforça sua observância, principalmente, quando a prova é volátil e facilmente adulterada ou destruída como nos crimes informáticos, reforçando ainda mais a necessidade de sua observância, sob pena de nulidade da prova ou da sua impossibilidade de valoração[249].

Em outras palavras, diante do avanço da tecnologia, resta evidente a importância da evidência eletrônica, pois ao mesmo tempo que a internet e o acesso aos computadores possibilitaram o uso de diversas ferramentas para a coleta e produção de provas, também representam um meio para a prática de crimes cibernéticos em todas as regiões do país.

Por conseguinte, em razão desses rastros deixados pela utilização de quaisquer meios eletrônicos, é necessário a criação de um banco de dados para investigações futuras. Isso porque a dispersão (uma das características da prova digital) pode fazer com que tais evidências desapareçam. Sabe-se que a velocidade com que os meios são transmitidos denotam a necessidade de adoção de medidas diferentes daquelas tradicionalmente impostas em relação às provas em geral.

Emerson Wendt destaca que:

---

[248] Exemplo já tratado no artigo "Combate à pornografia infantil", disponível em Estudos e Pesquisas em Direito sob o prisma do humanismo, da Editoria Universitária FDSBC.
[249] MOURA, Grégore Moreira de. **Curso de Direito Penal Informático**. Belo Horizonte, São Paulo: D'Plácido, 2021, p. 314-315.

> A partir da identificação e localização do computador que permitiu a conexão e o acesso criminoso na internet surge a denominada fase de campo, quando há necessidade de deslocamento de agentes policiais para realização de diligências com o intuito de promover o reconhecimento operacional no local. Essa diligência deverá ocorrer sempre de maneira discreta, pois poderá haver a necessidade de solicitar uma medida processual penal cautelar, em regra a representação para que o Poder Judiciário conceda o mandado de busca e apreensão. Ela ocorrerá de imediato nos casos de identificar o endereço que corresponde a uma residência e/ou rede corporativa[250].

Ainda, Domingos e Röder tecem o seguinte exemplo:

> Nos delitos cibernéticos de disseminação de pornografia infantil via web, é comum que no bojo dessas investigações em determinado país sejam identificados IP's e dados de conexão utilizados na prática criminosa de usuários de Internet pertencentes a outro país. Situação em que a polícia desse país envia as informações para o país onde os IP's identificados são alocados para que as investigações sejam desenvolvidas com relação às imagens e vídeos disseminados a partir desse local, tanto por ser de atribuição do país investigar e processar os delitos cometidos a partir de seu próprio território, quanto por ser mais provável que o criminoso seja identificado no local de onde disseminou as imagens e vídeos. Nesses casos, em que há a troca pelas autoridades competentes de diferentes estados de informações relevantes às investigações que ocorrem em geral por intermédio da INTERPOL, há a presunção de regularidade na obtenção e transmissão de tais informações conforme a legislação do país de origem. No entanto, afigura-se prudente que os investigadores submetam a prova ao Judiciário para validação e autorização de uso[251].

A complexidade das evidências em delitos cibernéticos, além de sua circulação internacional, demanda uma ação rápida e decidida na coleta e no armazenamento dessas provas. Tal como ocorre nos crimes convencionais, a manutenção da integridade da cena do crime é fundamental para o êxito da investigação e dos desdobramentos legais, e isso se aplica igualmente aos crimes digitais. Nos delitos cibernéticos, a necessidade de manter a integridade das informações é crucial para uma eventual punição, uma vez que a rápida circulação e as constantes transações de dados na internet, além da capacidade dos infratores de eliminar ou esconder informações de forma rápida, podem resultar em falta de responsabilização[252].

Diante disso, é fundamental garantir que a evidência eletrônica inclua mecanismos de certificação, autenticidade e integridade para que seja aceita como prova válida. Para tanto, é essencial que seja íntegra, para não ser questionada no tribunal quanto à sua legalidade.

---

[250] WENDT, Emerson. **Crimes Cibernéticos: ameaças e procedimentos de investigação.** 2. ed. Rio de Janeiro: Brasport, 2013, p. 53-54.

[251] DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schreiner. Obtenção de provas digitais e jurisdição na internet. **Crimes Cibernéticos: Coletânea de Artigos**. Ministério Público Federal. v. 3, 2018, p. 247-248.

[252] MOURA, Grégore Moreira de. **Curso de Direito Penal Informático**. Belo Horizonte, São Paulo: D'Plácido, 2021, p. 50.

3.7 A FORENSE DIGITAL EM NUVEM: EVIDÊNCIAS CRIMINAIS ELETRÔNICAS E SUA COLETA

Atualmente, é indissociável a análise de quaisquer campos do direito sem a ingerência da internet. Aliás, o que se vê é o surgimento da metarrealidade, em velocidade avassaladora, num compasso que, evidentemente, os modelos tradicionais de estrutura de investigação, notadamente no campo penal, não são mais passíveis de ingerência em tais casos.

Em consequência, as empresas cada vez mais globalizadas e, visando redução de custos e celeridade, possuem seus dados armazenados em nuvem (*cloud system)*. No entanto, se à primeira vista isto parece ser primoroso, um olhar mais atento faz incutir incertezas que, no campo do direito, podem gerar inseguranças jurídicas insanáveis.

Ora, se a empresa detentora de tais dados permanece em outro local, uma investigação poderá ser demasiadamente lenta, inviabilizando a proteção do bem jurídico penalmente tutelado.

O avanço contínuo das tecnologias oferece uma gama crescente de ferramentas valiosas para diversos perfis de usuários. A computação em nuvem é um exemplo desse recurso inovador. Essa tecnologia permite acessar arquivos, softwares, documentos e realizar uma variedade de tarefas pela internet[253].

Bomfati e Kolbe destacam que:

> [...] Uma das principais vantagens é a possibilidade de acessar esses dados em qualquer lugar e de qualquer dispositivo, desde que conectado à internet, sem a necessidade de estar no do usuário.
> Os serviços, programas, arquivos etc. ficam disponibilizados na nuvem, ou seja, em servidores que têm como principal função a de hospedar essas funcionalidades na internet. Grande parte desses servidores podem estar localizados em outros países, inclusive além fronteira, e são passíveis de serem acessados de forma remota. Podemos imaginar, de uma perspectiva simplista, que o sistema funciona como se o disco rígido do internauta não estivesse em seu dispositivo, mas localizado em lugares que muitas vezes o usuário desconhece, na nuvem. Um exemplo dessa ferramenta é o *Dropbox*, que, além de ter seus arquivos disponibilizados na nuvem, seus dados ficam duplicados no dispositivo hospedeiro.
> Apesar desse recurso ser muito utilizado por diferentes perfis de usuários, é uma tecnologia que dificulta (e muito) as investigações, pois é extremamente difícil de se apreender um servidor que esteja em outro país ou, na melhor das hipóteses, pode haver uma demora das plataformas em prestar as informações necessárias. Além disso, esses servidores são morosos em retirar do ar os sites solicitados, dificultando os serviços investigativos e tornando-se, assim, uma ameaça à segurança[254].

[253] BOMFATI, Cláudio Adriano; KOLBE, Armando Júnior. **Crimes cibernéticos**. Curitiba: Intersaberes, 2020, p. 165.
[254] Ibid., p. 165-166.

Tais fatos, contudo, encontram outro óbice: a questão do sigilo de dados e proteção aos interesses individuais.

De proêmio, é certo que não se pretende explorar exaustivamente todas as ferramentas de investigação e evidências geradas pelas tecnologias, uma vez que são numerosas e em constante evolução. O objetivo é ponderar questões relevantes nos métodos mais comuns e significativos que emergiram nesse contexto, notadamente levando-se em consideração o âmbito empresarial.

Inicialmente, é importante destacar que o armazenamento em nuvem é um modelo de computação que permite o armazenamento de dados e arquivos por meio de provedor, podendo ser privado, público ou híbrido. Nesse sentido e, diante da volatidade desses dados, surge a necessidade de analisar a investigação dentro desse sistema.

Ao analisar toda a historicidade do tema, vê-se que:

> [...] a forma de usar esses recursos mudou muito nos últimos anos com a Internet. É cada vez mais comum que os dados não fiquem mais armazenados no computador do usuário, sendo gravados e consultados a partir da Rede Mundial de Computadores, desde *websites* como o Wikipedia, que sempre estão disponíveis para consultas esporádicas, até serviços de armazenamento em nuvem, para manter seus arquivos salvos e seguros. Muito da vida e trabalho dos usuários hoje estão na nuvem (ou *cloud*).
> Tal situação abre outra fonte de dados no meio digital: *dados gravados em servidores da internet, externos ao dispositivo do usuário*. O acesso direto aos equipamentos e memórias envolvidos na computação em nuvem é particularmente difícil. Isso porque os equipamentos são configurados para atuar de forma compartilhada, replicada e redundante.
> Sendo assim, as informações de um determinado usuário podem estar divididas entre vários equipamentos ou sendo movidas sob demanda em questão de segundos para garantir a disponibilidade do serviço. Nesses casos, há praticamente uma impossibilidade de acessar fisicamente o equipamento para periciar informações, sendo o acesso via conexão de dados o único caminho viável para se obter as informações necessárias[255].

As formas de colaboração entre a Polícia Judiciária, o Ministério Público e o Poder Judiciário para combater crimes cibernéticos são determinadas pela legislação vigente em cada nação.

Dessa forma, é importante demonstrar como são realizados os procedimentos iniciais (fase de inquérito) nos casos de crimes cibernéticos.

Inicialmente, tem-se o procedimento técnico, no qual ocorre a notícia do crime (cibernético), e o delegado coleta informações fornecidas, analisando a ordem cronológica de

[255] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed.São Paulo: Revista dos Tribunais, 2024, p. 34.

como os acontecimentos ocorreram. Nesta etapa, é de suma importância obter o maior número de informações (telefone, e-mail, sites, chave pix, endereço, dentre outros). Ao identificar o possível local onde está o dispositivo responsável pela ação criminosa on-line, deve haver a quebra do sigilo de dados telemáticos e, após a obtenção do endereço IP, inicia-se a próxima etapa, de campo, na qual os policiais realizam investigações, verificando se trata-se, por exemplo, de residência ou estabelecimento comercial, além de análise sobre quem são as pessoas envolvidas e, nesse diapasão, reunir todas as informações importantes, tudo de maneira cautelosa – e discreta – evitando assim possíveis falhas em futuras diligências e na busca pelo culpado, afinal, não se pode esquecer das diversas características da prova digital, notadamente a volatilidade, que demandam todo esse cuidado[256].

E, aqui, o processo de custódia envolve o acompanhamento de vestígios, registrando as informações relevantes em banco de dados, estabelecendo uma sequência temporal.

A partir desse conceito surgem os procedimentos de custódia envolvendo crimes virtuais, abordando a coleta de evidências e os diferentes tipos de vestígios que podem indicar a prática de um crime cibernético, os quais poderão servir como prova durante o processo legal.

Um dos elementos eletrônicos mais importantes, que por si só pode embasar medidas cautelares ou até mesmo uma condenação, são os registros de Login (*logs*) mantidos pelas empresas de telecomunicações. Esses registros contêm informações cadastrais do usuário que estava conectado à rede de computadores, que geram diversos números vinculados ao dispositivo utilizado, funcionando de forma análoga a um CPF ou CNPJ (e, aqui, a evidência do DNA digital outrora mencionado). Além disso, fornecem dados como nome do usuário, data, horário de conexão e localização da máquina utilizada para o suposto crime. Outra evidência importante é o diretório de cache, que armazena informações sobre os sites visitados, assim como o histórico de navegação[257].

Após toda a coleta desses elementos, é de suma importância a elaboração do relatório pela polícia, o qual tem fé pública, podendo ser usado para oficializar a existência de um determinado site com informações ou documentos eletrônicos relevantes.

Emerson Wendt destaca o seguinte exemplo:

> Um passo que pode favorecer que se chegue ao autor desse tipo de crime é obter informações sobre o usuário de internet que promoveu a publicação do conteúdo pornográfico [...]

[256] WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos** – Ameaças e procedimentos de investigação. 3. ed. Rio de Janeiro: Brasport, 2021, p. 76-77.
[257] Ibid., p. 77.

> Outro aspecto que merece ser considerado é a possibilidade de o criminoso ter em sua residência ou local de trabalho computadores ou mídias contendo pornografia infantil. Em razão desse fato, é necessário apreender todo tipo de equipamento de informática considerado suspeito, ou seja, que possa ser utilizado para armazenar esse tipo de conteúdo. São exemplos desse recurso: HD externo, CD, DVD, *pen drives*, cartões de memória, aparelho celular etc.
> O monitoramento do e-mail ou da conexão de internet (pelo seu IP e/ou acesso telefônico) do usuário de computador pode ajudar, com acertada eficácia, a comprovação de uma relação com a pornografia infantil. Com o dispositivo e o software adequados, pode-se fazer esse monitoramento, previsto em lei, inclusive na *deep web*.
> É interessante acrescentar que criminosos com esse tipo de desvio de conduta procuram realizar atividades que permitam que tenham contato com suas potenciais vítimas e, no âmbito da internet, esse tipo de comportamento se repete. Além disso, as redes sociais representam verdadeiras "vitrines" para esses criminosos escolherem suas vítimas, que dificilmente fazem ideia do perfil psicológico desse tipo de pessoa.
> [...] Em um caso de cena de sexo explícito com crianças e adolescente em um ambiente virtual sob suspeita e investigação, destacamos como fundamentais, dentre outros aspectos já considerados, as seguintes atividades prévias de preservação de evidências:
> - Identificação da URL e/ou direcionamento de links, com consequente verificação de responsabilidade de domínio e hospedagem;
> - Coletar todas as informações disponíveis sobre o responsável pela postagem, como e-mails, links e *nicknames* envolvidos;
> - Captura da imagem da tela e, caso possível, cópia do conteúdo do site com o uso do software HTTrack [...]
> - No caso de vídeo, imediato *download* do arquivo ou realização de captura de *streaming* de vídeo, exibido através de algumas ferramentas disponíveis na web (VDownloader, Debut Video Capture, Camtasia, etc.);
> - Após essas medidas, pode-se solicitar formalmente ao provedor de conteúdo que, além de preservar as evidências para fins de instrução de investigação criminal, retire o conteúdo criminoso do ar, sob pena de incorrer em crime, substituindo a página por uma com informações oficiais sobre a investigação e ordem judicial;
> - Finalmente, e nos casos de provedor de conteúdo localizado em solo brasileiro, representar ao juízo para que, dentre outras medidas possíveis, o responsável pelo armazenamento do conteúdo ilegal detectado encaminhe, em uma mídia não regravável, o conteúdo da página ou URL investigada, dados cadastrais de usuários, *logs* de criação e de acesso subsequentes, com informações sobre eventuais alterações do conteúdo investigado[258].

A investigação dos crimes informáticos passa por três momentos, considerando o local de análise e o desenvolvimento dos atos criminosos. Segundo Grégore Moreira:

> [...] a *surface web* é a camada por nós utilizada da internet, através da navegação em que as páginas de acesso estão indexadas por buscadores, além de termos o serviço chamado de DNS (*Domain Name System)*, o que permite um tipo de investigação aberta, além da descoberta de dados deixados por registros de conexão e acesso, sendo que os rastros deixados são mais fáceis de detecção.
> Por outro lado, na *deepweb* não há indexadores de busca, o acesso é feito por VPN ou *softwares* específicos. Dentro dessa camada profunda da *web* encontramos a *dark web*, onde a criminalidade é muitas vezes obscura e organizada.
> Neste cenário, a dificuldade investigativa é muito maior, já que os rastros deixados são mínimos pelo uso constante de técnicas e *softwares* para ocultar IP, criptografias ponta a ponta, uso de redes virtuais privadas (VPN), o que aumenta sobremaneira a

[258] WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos** – Ameaças e procedimentos de investigação. 3. ed. Rio de Janeiro: Brasport, 2021, p. 76-77.

> dificuldade de apuração dos fatos, bem como a identificação da autoridade e materialidade[259].

Vê-se, portanto, que entender como são formadas as evidências eletrônicas é de suma importância, notadamente quando trata-se de um provedor estrangeiro que não possui escritório de representação no país e é aqui que temos que traçar parâmetros de cooperação internacional jurídica, especialmente por ser o Brasil signatário do *Mutual Legal Assistence Treaty* (MLAT), com representação pela concessão das medidas investigativas, que será objeto de análise mais adiante.

Em relação a todos os procedimentos acerca da documentação da prova, uma das maiores referências é a ABNT NBR ISSO/IEC 27037;2013, que apresenta um conjunto de orientações e processos destinados a uniformizar a manipulação de evidências digitais, a fim de aumentar sua aceitação, valor probatório e credibilidade na apresentação dos dados. Essas abordagens práticas são reconhecidas globalmente para sistematizar as etapas relacionadas à evidência digital, desde a coleta da fonte original, passando pela sua avaliação e análise, até a fase de apresentação[260].

Assim, tem-se o isolamento, a coleta, a preservação e, quanto às tecnologias de preservação digital, inicialmente o Código Hash, que é um processo algorítmico que gera uma cadeia curta de caracteres (geralmente entre 32 e 256) a partir do conteúdo de um arquivo específico. Se houver qualquer modificação nesse conteúdo, a cadeia de caracteres se altera significativamente. Em relação à sua aplicação como evidência digital, é crucial que o algoritmo seja resistente a colisões, ou seja, a ocorrência em que dois arquivos distintos podem gerar um mesmo código[261].

Acerca da integridade, existe meios que podem alterar a integridade do conteúdo, como:

> - abrir o arquivo e salvar, mesmo sem ter feito nenhuma alteração (rotacionar uma imagem e salvar, por exemplo);
> - enviar imagens ou vídeos através de aplicativos de mensagens, redes sociais ou mídia (as plataformas comprimem os conteúdos por padrão);
> - comprimir documentos PDF, vídeos ou imagens para reduzir o tamanho;
> - recortar trechos ou inserir qualquer elemento no interior do arquivo[262].

Da mesma forma, também existem outras alterações que não alteram a integridade do arquivo:

---

[259] MOURA, Grégore Moreira de. **Curso de Direito Penal Informático**. Belo Horizonte, São Paulo: D'Plácido, 2021, p. 285.
[260] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed. São Paulo: Revista dos Tribunais, 2024, p. 55.
[261] Ibid., p. 59-60.
[262] Ibid., p. 61.

- comprimir com pacote de arquivos como ZIP, RAR e outros;
- enviar arquivos por e-mail.;
- transportar com pendrives ou HD externos;
- salvar em drives na nuvem (Google Drive, OneDrive...)
- compartilhar por link[263].

Os procedimentos corretos para garantir a idoneidade e integridade dos dados extraídos são necessários para garantir que não resulte na quebra da cadeia de custódia e, consequentemente, na inadmissibilidade da prova digital, salientando o princípio da mesmidade, que visa assegurar a confiabilidade da prova. Nesse sentido, o STJ, no AgRg no HC 828054/RN, julgado em 23/4/2024, de relatoria do Min. Joel Ilan Paciornik, assim decidiu:

> PROCESSUAL PENAL. AGRAVO REGIMENTAL NO HABEAS CORPUS. TRÁFICO DE DROGAS. APREENSÃO DE CELULAR. EXTRAÇÃO DE DADOS. CAPTURA DE TELAS. QUEBRA DA CADEIA DE CUSTÓDIA. INADMISSIBILIDADE DA PROVA DIGITAL. AGRAVO REGIMENTAL PROVIDO.
> 1. O instituto da cadeia de custódia visa garantir que o tratamento dos elementos probatórios, desde sua arrecadação até a análise pela autoridade judicial, seja idôneo e livre de qualquer interferência que possa macular a confiabilidade da prova.
> 2. Diante da volatilidade dos dados telemáticos e da maior suscetibilidade a alterações, imprescindível se faz a adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios, de forma que seja possível a constatação de eventuais alterações, intencionais ou não, dos elementos inicialmente coletados, demonstrando-se a higidez do caminho percorrido pelo material.
> 3. A auditabilidade, a repetibilidade, a reprodutibilidade e a justificabilidade são quatro aspectos essenciais das evidências digitais, os quais buscam ser garantidos pela utilização de metodologias e procedimentos certificados, como, e.g., os recomendados pela ABNT.
> 4. 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 dados do arquivo digital.
> 5. De relevo trazer à baila o entendimento majoritário desta Quinta Turma no sentido de que "é ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia" (AgRh no RHC n. 143.169/RJ, relator Ministro Messod Azulay Neto, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, DJe de 2/3/2023).
> 6. Neste caso, não houve a adoção de procedimentos que assegurassem a idoneidade e a integridade dos elementos obtidos pela extração dos dados do celular apreendido. Logo, evidentes o prejuízo causado pela quebra da cadeia de custódia e a imprestabilidade da prova digital[264].

---

[263] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed. São Paulo: Revista dos Tribunais, 2024, p. 61.

[264] BRASIL. Superior Tribunal de Justiça. **AgRg no HC nº 828.054/RN**, Rel. Min. Joel Ilan Paciornik, julgado em 23/4/2024. Disponível em https://processo.stj.jus.br/SCON/pesquisar.jsp?pesquisaAmigavel=+%3Cb%3EHC+828.054%3C%2Fb%3E&b=ACOR&tp=T&numDocsPagina=10&i=1&O=&ref=&processo=&ementa=&nota=&filtroPorNota=&orgao=&rel

Também existe a certificação digital, tecnologia criptográfica que possibilita a assinatura de documentos eletrônicos de forma segura, utilizando chaves públicas e privadas. O processo inclui a atribuição de uma chave privada vinculada a um certificado criptográfico a um indivíduo ou organização específica, permitindo que essa pessoa ou entidade assine documentos usando essa chave. Em seguida, é viável conferir a autenticidade e a origem da assinatura utilizando as chaves públicas do certificado digital relacionado. Assim, conta-se com um sistema que facilita a posse de identidades digitais, permitindo também um método público para validar essa identidade em documentos, acesso a sistemas e outras aplicações. A validação de um documento digital envolve, inicialmente, o cálculo do código HASH referente ao seu conteúdo, seguido da aplicação de um processo criptográfico sobre esse código. Isso possibilita a confirmação da identidade do signatário e assegura a integridade do documento, oferecendo a certeza de que ele não sofreu modificações após a assinatura[265].

Por derradeiro, a tecnologia blockchain trata-se de tecnologia que executa duas funções principais: uma análise rápida para identificar alterações nos dados e a correção automática com base em replicações dessas informações. Essa abordagem assegura que os dados permaneçam imutáveis, impedindo alterações no conteúdo previamente inserido. Ao adicionar um novo bloco de dados, é gerada uma "impressão digital" (código HASH) do bloco anterior, que é então armazenada junto ao novo bloco, formando uma "cadeia de blocos" (de onde vem o termo blockchain). Esse processo torna mais fácil a detecção de mudanças dentro do conjunto de dados, uma vez que, se um deles for alterado, o restante não se alinha mais[266].

Acerca da ISO/IEC 27037, que fornece recomendações acerca da prova digital (*digital evidence)*, tendo por finalidade padronizar o tratamento de evidências digitais, que é sustentada por três pilares:

> Relevância: a evidência digital é considerada relevante quando se destina a provar ou refutar um elemento de um caso específico que está sendo investigado.
> Confiabilidade: Este termo define a evidência digital quando “para garantir que a evidência digital seja o que pretende ser”.
> Suficiência: O conceito de suficiência significa que a evidência digital seja suficiente para permitir que elementos questionados sejam adequadamente examinados ou investigados[267].

---

ator=&uf=&classe=&juizo=&data=&dtpb=&dtde=&operador=e&thesaurus=JURIDICO&p=true&livre=HC+828.054. Acesso em 27 jul. 2024.

[265] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. ed. São Paulo: Revista dos Tribunais, 2024, p. 61-62.

[266] Ibid., p. 63.

[267] OLIVEIRA, Vinícius Machado de. ABNT NBR ISO/IEC 27037:2013. **Academia Forense Digital.** Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/. Acesso em: 8 out. 2024.

Também dispõe sobre os componentes de identificação, coleta e preservação, o que reafirma como a prova digital, hoje, é tratada com mais acuidade, dada sua importância.

3.8 CONSIDERAÇÕES SOBRE O PROJETO DE LEI 4.939/2020

Como visto, no ordenamento jurídico brasileiro são admitidos todos os meios probatórios desde que legalmente e moralmente legítimos[268]. Além disso, como já destacado, a Constituição Federal veda a utilização de provas ilícitas no sistema penal.

Isto posto, em interpretação conjugada, vê-se que é essencial que a prova que seja obtida por meio eletrônico seja lícita.

Por tal razão, tramita no Congresso Nacional o PL 4.939/20, que trata sobre as normas de obtenção e admissibilidade de provas digitais na investigação e no processo (art. 1º), visando aprimorar processos sobre crimes cibernéticos.

Aliás, assim consta de sua justificação:

> A forte influência que a tecnologia vem exercendo sobre o modo de viver do ser humano tem provocado, também, intensa alteração na constituição e regulação dos fatos jurídicos contemporâneos.
> Contratos eletrônicos, moedas virtuais e relações sociais digitais se tornaram de tal forma presentes e relevantes na sociedade a ponto de fazer anacrônica a legislação disponível. Tal circunstância tem gerado grandes dúvidas sobre o correto entendimento e tratamento destas realidades modernas e cambiantes, trazendo insegurança jurídica e angústias.
> Em paralelo, instituiu-se ao longo dos últimos 20 anos uma diversidade de normas visando, de algum modo, adaptar o regramento diante das novas possibilidades, o que ocorreu na medida em que vieram surgindo.
> [...] No plano penal, temos gerado paulatinamente no ordenamento diversos tipos penais cuja matriz factual é de ordem tecnológica, tais como as alterações provocadas pela Lei 12.737/12, a par de outras advindas de outras legislações.
> Em 2018, a Internet era utilizada em 79,1% dos domicílios brasileiros [...] Consequentemente, a migração massiva das relações sociais para o meio eletrônico tem o substancial efeito de digitalizar os conflitos, matéria-prima do Direito.
> De fato, a forma dos negócios jurídicos, e mesmo da prática de ilícitos civis e penais, sofreu grande transformação em um curto período, a fazer desafiar a adaptabilidade do Direito que, agora, precisa ainda reconhecer a existência e necessidade de proteção maior de direitos fundamentais que decorrem da própria existência de um mundo cibernético.
> Esta realidade, inexorável e galopante, torna fundamental prover uma resposta aos anseios sociais quanto a uma norma capaz de regular as novas peculiaridades e bens jurídicos advindos da evolução tecnológica de um modo mais uniforme[269].

---

[268] Nesse sentido, o artigo 369 do Código de Processo Civil estabelece que: "As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz".

[269] BRASIL. PL 4.939/20. Dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências. Brasília, 2020. Disponível em:

Inclusive, há a definição de prova digital, sendo *toda informação armazenada ou transmitida em meio eletrônico que tenha valor probatório* (art. 4º) e, além disso, que às provas digitais serão aplicadas, subsidiariamente, todas as disposições atinentes às provas em geral (parágrafo único do citado artigo).

Outro ponto interessante é o estabelecimento dos meios de obtenção da prova digital, como a busca e apreensão de dispositivos eletrônicos e outros meios de armazenamento de informação e coleta remota (art. 9º)[270].

Também denota como ocorrerá a decisão judicial para tanto. Nesse sentido, importante destacar que determina a necessidade de descrição dos fatos investigados, além dos motivos, indicando a necessidade da diligência, os limites e o prazo (art. 13)[271].

Além disso, salvaguarda dados íntimos e determina restrições de acesso à informação que serão apartados em autos próprios (art. 24)[272].

Como se vê, o projeto estabelece *meios de prova* (busca e apreensão de dispositivos eletrônicos, sistemas informáticos ou outros meios de armazenamento de informação eletrônica, coleta remota, coleta por acesso forçado e tratamento de dados disponibilizados em

---

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node08pwjhswz835euh8tzvacb7on17491799.node0?codteor=1936366&filename=PL+4939/2020. Acesso em: 10 out. 2024.

[270] Art. 9º Constituem meios de obtenção da prova digital, na forma da Lei: I – a busca e apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, e o tratamento de seu conteúdo. II – a coleta remota, oculta ou não, de dados em repouso acessados à distância. III – a interceptação telemática de dados em transmissão. IV – a coleta por acesso forçado de sistema informático ou de redes de dados. V – o tratamento de dados disponibilizados em fontes abertas, independentemente de autorização judicial.

[271] Art. 13. A ordem judicial para obtenção da prova digital para fins de investigação e processo penal descreverá os fatos investigados com a indicação da materialidade e possível autoria delitiva, indicando ainda os motivos, a necessidade e os fins da diligência, estabelecendo os limites da atividade a ser empreendida e o prazo para seu cumprimento. § 1º Em caso de monitoramento do fluxo de dados, o prazo da medida não poderá exceder a 60 (sessenta) dias, permitidas prorrogações por igual período, desde que continuem presentes os pressupostos autorizadores da diligência, até o máximo de 360 (trezentos e sessenta) dias, salvo quando se tratar de crime permanente, enquanto não cessar a permanência. § 2º A obtenção da prova digital pode se dirigir a uma terceira pessoa, desde que haja indícios de que o investigado utilize o dispositivo eletrônico, ou quaisquer outros meios de armazenamento de informação eletrônica, com ou sem o conhecimento do proprietário. § 3º O órgão de investigação ou o Ministério Público poderá requisitar a guarda da prova digital sem acesso ao conteúdo pelo prazo de 1 (um) ano, independentemente de autorização judicial, quando houver perigo na demora, devendo comunicar a medida ao juiz competente em até 24 (vinte e quatro) horas, para validação da medida.

[272] Art. 24. Os dados pessoais sensíveis, íntimos ou sigilosos do investigado, acusado ou pessoas a ele relacionadas, que sejam relevantes ao caso, mas que não digam respeito aos demais sujeitos processuais, serão apartados em autos próprios, mantendo-se acessíveis apenas aos interessados, vedada a alteração do espelhamento.

§ 1º Decorridos 05 (cinco) anos do cumprimento integral da sentença condenatória ou em caso de absolvição ou de decretação de extinção de punibilidade, os dados mencionados no caput serão indisponibilizados, desde que não haja interesse público na preservação ou que não tenha relevância ou pertinência processual, devendo ser intimados os interessados e atualizada a garantia de integridade e anterioridade dos dados remanescente.

§ 2º Os dados que se enquadrem nas restrições de acesso à informação, nos termos da Lei, serão apartados em autos próprios e encaminhados em 24 (vinte e quatro) horas à autoridade competente, vedada a alteração do espelhamento.

fontes abertas), *interceptação telemática*, *infiltração de agentes* em redes de dados, *ação disfarçada*, *coleta forçada*, *preservação de dados pessoais*, além de estabelecer *novos crimes*.

Assim, de acordo com a proposta, prova eletrônica se refere a qualquer dado armazenado ou enviado através de meios digitais, que possua validade como evidência, devendo ser aplicadas a elas, de forma complementar, as mesmas normas referentes às evidências em geral.

Hoje, os contratos on-line, criptomoedas e interações sociais na internet são tão comuns e importantes para a sociedade que, de certa forma, tornaram obsoleta a legislação atual. Dessa forma, conforme o plano, os indivíduos autorizados poderão solicitar autorização judicial para armazenar e acessar dados digitais em posse de terceiros, com o intuito de investigação ou instrução processual, desde que sigam os critérios de relevância, eficácia e equilíbrio.

Por conseguinte, as empresas responsáveis pela infraestrutura, conexão e serviços on-line devem manter, além das informações exigidas por lei, os registros de dados essenciais para identificar claramente os usuários de seus serviços por determinado período.

Hoje, existem diversas empresas de tecnologia que recebem tais comunicações privadas reguladas pela lei daquele país, não podendo simplesmente entregar as informações para o Brasil sem um pedido formal. Essa é, portanto, a questão que tem aparecido em investigações criminais e que tratam da proteção de dados num aspecto jurisdicional de competência do Estado brasileiro.

Ademais, a lei disciplina como ocorrerá a interceptação telemática (art. 10), a questão da requisição itinerante (art. 11), a coleta por acesso forçado (art. 13), e elenca a cadeia de custódia digital específica, com “ambiente controlado com redução de contaminação”, “espelhamento técnico em duas cópias, com o máximo de metadados e a descrição completa de procedimentos, datas, horários ou outras circunstâncias de contexto aplicáveis” e “preservação imediata após o ato de espelhamento com emprego de recurso confiável que garanta a integridade da prova” (art. 19).

São apenas alguns exemplos que denotam hoje a importância de diploma específico acerca do tema haja vista a constante interpretação entre as linhas que demarcam o processo analógico-digital que, no mais, pode ocasionar inseguranças jurídicas e invalidações das provas.

3.9 A PROBLEMÁTICA DA INVESTIGAÇÃO CRIMINAL NA *DEEP WEB* E *DARK WEB*

Concomitantemente a todos os progressos, as atividades ilícitas no ambiente digital também se expandiram.

A internet é dividida, basicamente, em duas partes, quais sejam, a *surface web* e a *deep web*. A primeira é aquela acessível a todos, por meio dos programas padrão de navegação, ao passo que a segunda abrange espaço maior, com dados não registrados, daí porque o acesso é mais difícil. Indo além, chega-se à *dark web*, segmento ainda mais escondido, sendo necessário inclusive programas específicos para acessá-lo.

Nesse sentido:

> A *surface* é constituída, basicamente, por páginas, sites e conteúdos que utilizam a arquitetura de redes cliente/servidor, onde existem computadores "especiais" encarregados de prover serviços aos seus clientes. Essas máquinas hospedam páginas *web*, serviços de e-mail, banco de dados, arquivos e muitos outros serviços utilizados diariamente por pessoas e empresas.
> [...]
> A *deep web* é, portanto, composta por redes de computadores que têm como características o anonimato, a criptografia, a descentralização e a codificação aberta, e cujo conteúdo não é "visível" pelas ferramentas de busca convencionais. A arquitetura de redes predominante é a ponto a ponto (P2P), ou seja, dispensa um servidor central, cenário no qual todos os componentes (pontos ou nós) funcionam ora como cliente, ora como servidor.
> O exemplo mais clássico de rede tipicamente dentro dos conceitos de *deep web* é a Tor. Nessa rede estão presentes as quatro características básicas listadas anteriormente e por isso ela é, muitas vezes, associada erroneamente ao próprio conceito de *deep web*. Por outro lado, redes utilizadas para o *download* de arquivos, como *torrents* e P2P, apresentam apenas uma ou outra dessas características. Mas não é possível classificar essas redes como pertencentes à *surface web*, já que seus respectivos conteúdos não estão indexados por lá, além de serem, em geral, totalmente descentralizadas. Resta-nos, portanto, inseri-las dentro dos conceitos da *deep web* ou então criar uma terceira classificação doutrinária, nominando-as como "redes descentralizadas".
> [...]
> Por outro lado, a *dark web*, ou *darknet*, é a rede da *deep web* ou parte dela com características de um alto grau de anonimato e segurança exigido e é utilizada, como regra, para o cometimento de ilícitos criminais e práticas escusas. É empregada por usuários de internet, ativistas políticos, *hackers* e criminosos, notadamente por garantia de privacidade nas comunicações e/ou a não aplicação da lei penal.
> A rede Freenet, por exemplo, possui essa função. Nesse modo de funcionamento, os usuários devem ser considerados "amigos de confiança" para, só assim, poderem fazer parte dela. Os demais usuários sequer saberão da existência desta *darknet*, tampouco qual o tipo de conteúdo compartilhado. Dessa forma, o conceito de *darknet* abrange não só o conteúdo altamente sensível (imoral, ilegal, secreto ou restrito a apenas um grupo de usuários), mas também o alto grau de anonimato e segurança exigidos pelos componentes dessa rede "obscura"[273].

Aqui está o cerne da discussão: de um lado, possibilita, entre outras vantagens, garantir a confidencialidade das interações entre usuários e acessar conteúdos, como artigos e blogs que não estão disponíveis na *surface web*; de outro, o anonimato pode ser utilizado para a realização de ações ilegais[274].

---

[273] BARRETO, Alesandro Gonçalves; SANTOS, Hericson dos. **Deep Web:** Investigação no submundo da internet. Rio de Janeiro: Brasport, 2019, p. 6-8.
[274] DUARTE, David; MEALHA, Tiago. **Introdução à deep web**. Lisboa: IET Working Papers Series, 2016, p. 2.

Ainda, os endereços localizados na *deep web* não são indexados e não podem ser acessados por ferramentas de busca como Google ou Bing. O endereço IP do usuário é mascarado, assim como suas outras informações pessoais. Há uma grande quantidade de dados disponíveis na *deep web*, o que significa que nem todos os usuários estão envolvidos em atividades ilícitas, desafiando a crença comum. É possível descobrir diversos tipos de informações, incluindo algumas questionáveis ou até mesmo ilegais[275].

Neste espaço, evidentemente, diversos crimes graves também são cometidos, como pornografia infanto-juvenil, racismo, venda de armas, drogas e até mesmo tráfico de órgãos e de pessoas.

Diante disso e, estando evidente a dificuldade quanto à identificação dos autores, a preocupação mundial resultou na Convenção sobre o Cibercrime, conhecida como Convenção de Budapeste, que indica a discussão de soluções visando a proteção da sociedade e tendo por objetivo a cooperação entre os Estados.

O problema reside na (ausência) de verificação no caso da *deep web* ou *dark web* pois aquele conteúdo que é retirado da internet pode permanecer nessas interfaces obscuras.

A *deep web* possibilita o armazenamento de informações cruciais para a preservação da rede, assim como dados confidenciais, cujo acesso é limitado apenas a quem detém o endereço e as credenciais adequadas. Exemplos incluem prontuários médicos, bases de dados acadêmicas, informações de segurança nacional, registros financeiros, entre outros. Frequentemente, a finalidade é resguardar ou controlar o acesso a dados e informações particulares[276].

Já a *dark web* é a parte da *deep web* que realmente abrange atividades ilegais ou criminosas, incluindo o tráfico de drogas, de seres humanos e órgãos, além de crimes como pedofilia e homicídios[277]. É, portanto, uma forma de navegação que visa a proteção da identidade dos usuários e das informações, criando evidentes obstáculos à localização das partes.

E, em contrapartida, como o Poder Legislativo não consegue acompanhar todos os avanços tecnológicos, a internet torna-se um cenário em que há evidente benefício no anonimato.

---

[275] MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 196.
[276] Ibid., p. 197.
[277] MARTINS, loc. cit.

Assim, a apuração e o combate aos delitos cibernéticos apresentam desafios significativos, uma vez que essas condutas podem acontecer em qualquer lugar, desde que o infrator tenha conexão à rede. Nesse cenário, a internet atua como uma importante ferramenta facilitadora para a execução desses crimes, devido à complexidade em identificar o autor da infração. Ademais, é fundamental que as investigações sejam conduzidas por especialistas qualificados, que possuam habilidades técnicas em informática.

4 O CONTEXTO EMPRESARIAL: DESAFIOS E IMPACTOS NA PROTEÇÃO DE DADOS

4.1 CONSIDERAÇÕES INICIAIS SOBRE CRIMES VIRTUAIS

Por muito tempo, falava-se na internet como um campo sombrio, ou "terra sem lei". No entanto, com sua crescente evolução – e, hoje, totalmente enraizada no cotidiano – é evidente que não poderia ser entendida como meio dissociado de leis, em que a liberdade seria irrestrita.

A web passou a fazer parte da vida comum, com crescimento exponencial, haja vista que a quase totalidade das interações sociais e profissionais são realizadas por intermédio da conexão e, nesse sentido, os crimes também passaram a ser praticados em referido meio. Nesse sentido, surgem os "crimes cibernéticos", "crimes digitais", "crimes informáticos", que são os atos ilegais envolvendo o uso indevido do ambiente digital como um todo.

Ora, se antes o criminoso tentava, de todas as formas, escapar de um confronto direto com a vítima sempre com o fim de evitar eventual punição, hoje pode utilizar-se da internet para praticar diversos atos sem nem sequer ter o risco de – ao menos em um primeiro momento – ser identificado. Aliás, com o avanço da Inteligência Artificial[278] (IA), o que se vê são adaptações que facilitam a prática de tais delitos. Como exemplo, recentemente, um funcionário do setor financeiro de uma multinacional foi induzido a pagar US$ 25 milhões a fraudadores que usaram *deepfake* com o fim de se passar pelo diretor em uma chamada de videoconferência[279]. É fato: a criminalidade assumiu novos contornos e, diante disso, a investigação penal também deve se adequar a esses novos panoramas.

Nesse sentido, Tarcísio Teixeira explica que:

> Podemos dizer que muitos dos crimes já existentes podem ser cometidos pela internet, por exemplo, furto, estelionato, calúnia, pornografia, entre muitos outros, utilizando

[278] Artificial Inteligence ou AI, é expressão cunhada no ano de 1956, por Hohn McCarthy para designar programa de computador que fosse capaz de fazer o que normalmente é a inteligência humana que faz. (AUGUSTO, Victor; VALENTE, Estevam. **Inteligência artificial e o Direito Penal:** o propósito da responsabilidade criminal em decorrência de sistemas tecnológicos altamente complexos nas empresas. Belo Horizonte, São Paulo: D'Plácido, 2023, p. 22).

[279] Segundo notícia, "o esquema elaborado levou o empregado a participar de uma chamada de vídeo com o que ele pensava ser vários outros membros da equipe, mas todos eles eram, na verdade, recriações de deepfake [...] Acreditando que todos os outros participantes da ligação eram reais, o trabalhador concordou em remeter um total de US$ 200 milhões de dólares de Hong Kong – cerca de US$ 25,6 milhões, acrescentou o policial. O caso é um dos vários episódios recentes em que se acredita que os fraudadores tenham usado a tecnologia deepfake para modificar vídeos e outras filmagens disponíveis publicamente para enganar as pessoas e tirar dinheiro". CHEN, Heather; MAGRAMO, Kathleen. Golpistas usam deepfake de diretor financeiro e roubam US$ 25 milhões. **CNN Brasil**, 05 fev. 2024. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/golpistas-usam-deepfake-de-diretor-financeiro-e-roubam-us-25-milhoes/. Acesso em: 31 de out. 2024.

> a rede mundial de computadores como instrumento de execução. Isso porque, via de regra, as características do tipo penal se referem à conduta ou omissão, não necessariamente à maneira como se deu a conduta[280].

O computador (aqui em sentido amplo, afinal, também se observa o uso de smarthphones*)* serve como ferramenta para cometer delitos. Esses crimes já são abrangidos pela legislação brasileira, incluindo infrações como danos ao patrimônio, fraudes, ofensas à honra, calúnia, invasão de privacidade, violação de correspondência e restrições à liberdade de comunicação, além de transgressões relacionadas à propriedade intelectual, como a infringência de marcas, patentes e direitos autorais[281].

Esses crimes são definidos como de informático impróprios, pois podem ser praticados de diferentes formas, sendo a internet apenas um dos meios. Em contrapartida, existem os crimes próprios, "atos contra o computador (ou seja, contra o próprio material informático, o computador propriamente dito e seus componentes e suportes [...]) e atos contra dados ou programas de computador"[282]. E, considerando todos os dados contidos nos provedores, o objetivo criminoso pode ser o acesso ao sistema computacional em si (como a invasão a determinado *website*) ou a utilização da internet como meio, a exemplo da prática de estelionato.

Os crimes cibernéticos estão ligados à obtenção de informações protegidas, de dados bancários e informações pessoais, ameaças, dentre outros. Tudo o que se pensava e se tratava como crime até então pode se revelar no âmbito digital com uma agravante: a identificação do agente é muito mais difícil, afinal, pode-se cometer tais delitos em qualquer lugar do mundo e por meio de qualquer computador, inclusive com alteração de IP.

Todas essas novas formas de cometimento de delitos não podem ser desconsideradas; ao contrário, denotam a necessidade de meios igualmente diferentes, visando a prevenção e repressão a tais crimes.

Tanto que tramita a PL 5.441/2020, que define diversos conceitos para efeitos penais acerca dos crimes cibernéticos e estabelece conceitos, como o sistema informatizado, dados informatizados, provedor de serviços, dados de tráfego e credencial de acesso[283]. Ainda,

---

[280] TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico**. 5. ed. São Paulo: Saraiva, 2020, E-Book, p. 694.
[281] Ibid., p. 293.
[282] TEIXEIRA, loc. cit.
[283] PL 5.441/2020, art. 1º. Para efeitos penais, considera-se: I – "sistema informatizado": computador ou qualquer dispositivo ou conjunto de dispositivos, interligados ou associados, em que um ou mais de um entre eles desenvolve o tratamento automatizado de dados informatizados através da execução de programas de computador, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informatizados armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos; II – "dados informatizados": qualquer representação de fatos, informações ou conceitos sob forma suscetível de processamento num sistema

estabelece delitos como acesso indevido a sistema informatizado (art. 2º), sabotagem informática (art. 3º), danos a dados (art. 4º), fraude (art. 5º), obtenção indevida de credenciais de acesso (art. 6º), além de elencar excludentes de ilicitude, quando as condutas são realizadas com os fins de investigação por agentes públicos no exercício de suas funções, pesquisa acadêmica devidamente autorizada e documentada, testes e verificações autorizadas de vulnerabilidade de sistemas ou desenvolvimento e manutenção para aperfeiçoamento de sistemas de segurança desde que, claro, autorizadas[284]. Portanto, verifica-se uma constante preocupação com as disposições legais acerca do tema que, infelizmente, não avança como deveria.

Fato é que, diante da prática de algum delito, será imperiosa a necessidade de investigação criminal, agora no meio digital.

No mundo da web, como se viu da análise do MCI, é dever dos provedores de conexão e de aplicação o armazenamento, guarda, tratamento de dados pessoais e de comunicações privadas, com adoção de padrões de segurança, por meio de controle sobre o acesso de dados, não deixando de lado a responsabilidade daqueles que terão acesso àqueles dados.

Mesmo com a popularização da internet na década de 1990, somente em 2012 foi criada lei específica para crimes cibernéticos, a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, em um episódio no qual teve fotos íntimas obtidas de seu computador e divulgadas na internet[285].

---

informatizado, incluindo programas de computador; III – "provedor de serviços": qualquer entidade, pública ou privada, que faculte aos utilizadores de seus serviços a capacidade de comunicação ou processamento por meio de seu sistema informatizado, bem como qualquer outra entidade que trate ou armazene dados informatizados em nome desse serviço de comunicação ou processamento ou de seus usuários, incluindo servidores de aplicação e de conexão; IV – "dados de tráfego": dados informatizados relacionados com uma comunicação efetuada por meio de um sistema informatizado, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo de serviço subjacente; V – "artefato malicioso": sistema informatizado, programa ou endereço localizador de acesso a sistema informatizado destinados a permitir acessos não autorizados, fraudes, sabotagens, exploração de vulnerabilidade ou a propagação de si próprio ou de outro artefato malicioso; VI – "credencial de acesso": dados informatizados, informações ou características individuais que autorizam o acesso de uma pessoa a um sistema informatizado.

[284]BRASIL, **PL 5.441/2020.** Define os crimes cibernéticos e dá outras providências. Câmara dos Deputados. Brasília, dezembro 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2266423ra.leg.br). Acesso em: 3 abr. 2024.

[285] "[...] a norma ganhou vida a partir da repercussão do que aconteceu com a atriz: em 2011, ela teve seu computador pessoal invadido e 36 fotos íntimas divulgadas em redes sociais após não ceder à extorsão dos criminosos". (ARAÚJO, Janaína. Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos. **Rádio Senado,** 29 mar. 2023. Disponível em https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos#:~:text=Conhecida%20como%20Lei%20Carolina%20Dieckmann%2C%20a%20norma%20ganhou%20vida%20a,ceder%20%C3%A0%20extors%C3%A3o%20dos%20criminosos. Acesso em: 31 de out. 2024.)

Como resultado, houve a alteração no Código Penal, com inserção dos crimes de invasão de dispositivo informático (art. 154-A[286]) e interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (art. 266[287]).

Imperioso ressaltar que o art. 154-A sofreu modificações em 2021 pela Lei nº 14.155, que tornou a reprimenda dos crimes de violação de dados, furto e estelionato envolvendo meios eletrônicos e dispositivos mais severa, evidenciando a resposta do legislador ao aumento de delitos praticados por meio eletrônico.

Ainda, o art. 155 do Código Penal (furto) foi acrescido dos seguintes parágrafos:

> § 4º-B – A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C - A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional

Além disso, passou a disciplinar a fraude eletrônica:

> Art. 171, §2º-A – A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio fraudulento, ou por qualquer outro meio fraudulento análogo.
> § 2º-B – A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

---

[286] Invasão de dispositivo informático. CP, art. 154-A – Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

[287] Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública. CP, art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

Após dois anos da aprovação da Lei nº 12.737/2012, foi criado o Marco Civil da Internet, por meio da Lei nº 12.965/2014, estabelecendo direitos e deveres dos usuários e dos provedores.

Posteriormente, a Lei nº 13.853/2018 (LGPD) estabeleceu novas regras para a proteção de informações digitais, com diretrizes acerca da proteção de dados.

De todo modo, o desafio é analisar o tratamento – e punição – dos crimes praticados em meio ambiente digital, notadamente no que diz respeito às provas sobre a materialidade delitiva e aos indícios de autoria que fornecem a justa causa para eventual ação penal.

Como obstáculos a serem superados, pode-se citar o alto custo e a ausência de infraestrutura, afinal, não é tarefa simples, tampouco de fácil armazenamento, diante de todas as características atinentes à prova digital, como a volatilidade.

4.2 AUTORREGULAÇÃO, GOVERNANÇA CORPORATIVA E COMPLIANCE

A ideia de compliance surge na legislação norte-americana com a criação da *Prudential Securities* (1950) e a regulação da *Securities and Exchange Comission* (SEC), com a finalidade de estabelecer procedimentos internos de controle e monitoramento das operações[288], o que revelou uma necessidade ainda maior com a globalização e consequente crescimento do comércio internacional.

Assim, o termo compliance vem do verbo *to comply*, ou seja, agir de acordo com um determinado comando. Dessa forma, irá orientar o comportamento daquela instituição, dentro do mercado e, não apenas isso, mas também a própria atuação dos funcionários.

Portanto, vê-se que é analisado de forma sistêmica, visando a preservação de valores éticos e a mitigação de riscos. Dessa forma:

> A importância dos programas de *compliance* para as empresas incrementou-se desde a edição do *SOX, Sarbanes-Oxley Act*, em 30 de julho de 2002, nos Estados Unidos da América, num momento em que a globalização parecia um movimento irreversível. [...]
> Apesar de sua origem bem mais antiga que o *Sarbanes-Oxley Act*, o certo é que, desde então, globalmente, os programas de *compliance* passaram, gradualmente, a fazer parte da política empresarial. Grandes empresas em todo o mundo passaram a adotar programas de *compliance*. Os motivos são tanto as obrigações surgidas nas legislações dos Estados ou mesmo decisões internas de autorregulação empresarial, inseridos nos

[288] BERTOCELLI, Rodrigo de Punho. Compliance. *In:* CARVALHO, André Castro; ALVIM, Tiago Cripa; VENTURINI, Rodrigo Bertoccell (cood.). **Manual de Compliance.** 2. ed. Rio de Janeiro: Forense, 2020, p. 40.

> seios das empresas, como sistemas de minoração de riscos ou mecanismos de autoproteção empresarial[289].

Os programas de conformidade surgiram, assim, tanto em decorrência de conflitos quanto pela convergência de interesses, promovendo um desenvolvimento constante. Tornaram-se instrumentos eficazes na mitigação de riscos corporativos, salvaguardando os bens das empresas, assim como os interesses dos empregados e da sociedade. Esses programas passaram a ocupar uma função no setor público em um contexto de instabilidade jurídica e incerteza – notadamente no âmbito penal - exigindo que as empresas adotem a autorregulação e reduzindo a necessidade de intervenção estatal na fiscalização[290].

A efetivação da LGPD, que complementa o MCI, está, de fato, gerando efeitos nas operações das empresas no Brasil, que vêm gradualmente se ajustando às novas exigências relacionadas à coleta e ao manuseio de dados, considerando que sua vigência começou em setembro de 2020, exceto no que diz respeito às penalidades administrativas[291].

Além das empresas que já existem se adequarem aos novos padrões de proteção de dados, as startups têm incorporado a privacidade como um valor fundamental desde a sua criação, conceito esse denominado como princípio de *privacy by design*[292].

Isso implica que desde os estágios iniciais de elaboração da empresa, são consideradas questões vinculadas à privacidade e à proteção das informações dos clientes ou usuários, assegurando a conformidade com a LGPD e outras regulamentações aplicáveis. A proposta é integrar medidas de proteção de privacidade e de dados pessoais em todos os projetos criados[293].

É autorregulação porque há um deslocamento da atividade que seria do Estado para outras empresas, que terão a possibilidade de encontrar caminhos que estejam relacionados à sua própria atividade. Nesse sentido:

> [...] o Compliance deve ser visto e percebido como uma forma de conscientizar os colaboradores e parceiros, por meio de reflexões, sentimentos reais e aprendizado. Ética, moral e comportamento adequado devem fazer mais parte do escopo da transformação de cultura, do que de práticas implementadas que visam perpetuação do comportamento da alta direção, que deverá emanar o exemplo aos seus subordinados e nas suas relações com os parceiros externos.
> Isso não significa que aspectos legais, regulamentações e eventuais sanções aplicáveis devam ser deixados de lado, pelo contrário, certamente são elementos que atuarão como fortes aliados no atingimento do objetivo maior: fazer o certo. Contudo, se

[289] SANTOS, Fábio Antônio Tavares dos. **Direito Penal Empresarial** – a responsabilidade penal horizontal**.** São Paulo: LiberArs, 2022, p. 46.
[290] Ibid., p. 47.
[291] MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 142.
[292] Ibid., p. 138.
[293] MARTINS, loc. cit.

> queremos disseminar uma cultura, precisamos ir além e criar mecanismos eficientes para transformar os indivíduos [...][294].

No Brasil, o seu marco legal surge com o advento da Lei n. 9.613/98 (Lei de Lavagem de Dinheiro), de modo que o compliance levará em conta as peculiaridades de cada atividade empresarial desenvolvida, implementando de forma conjunta toda a vigilância necessária com o fim de evitar o descumprimento do ordenamento[295].

Dessa forma, o compliance é a criação de normas internas cujo objetivo é apoiar a organização privada na observância das leis pertinentes. Em outras palavras, é a adoção de diretrizes internas focadas na autorregulação do ente privado em relação ao cumprimento das normas legais aplicáveis. A implementação de tais práticas ocorreu inicialmente como uma estratégia para prevenir a responsabilização penal, tanto da pessoa jurídica – se viável – como dos indivíduos que fazem parte de seu quadro. Assim, não se pode negar que a origem do compliance está intimamente ligada à área criminal[296].

Não se olvida, claro, que o compliance é mais amplo, versando, por exemplo, sobre temas tributários, ambientais e trabalhistas, mas a questão da responsabilização penal é evidente. Diante disso e com a adoção de regras privadas para tanto, estando aqui presente a autorregulação regulada. No entanto, é sempre necessária a atenção aos aspectos de Estado de Direito e, dentro desse espaço, a ideia de justificação da própria extensão do Direito Penal. Dito por outro modo, ao dizer que o Estado delega em parte atividade que pertence a ele, necessariamente essa delegação sofre consequências e o modo que realiza isso se dá por intermédio do *criminal* compliance, que busca estabelecer responsabilidades dentro do âmbito criminal em virtude dessa delegação que se desenvolve. Por isso é autorregulação regulada e, dentro disso, tem-se também a governança corporativa.

Os limites dessa governança ainda encontram-se em discussão recente e o Direito Penal, por si só, não é capaz de proceder ao enfrentamento, necessitando contar com o apoio de outros ramos do direito. Nesse sentido, a partir do momento em que se chega à conclusão de que o Direito Penal não é suficiente, alternativas podem surgir, como o direito administrativo sancionador e o direito de intervenção. Nessa esteira, o direito de intervenção surge porque

---

[294] FRANCO, Isabel. **Guia Prático de Compliance**. Rio de Janeiro: Forense, 2019. *E-book*, p.48. ISBN 9788530988692. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530988692/. Acesso em: 01 nov. 2024.

[295] BARBAS, Leandro Moreira Valente; DEVEIKIS, Gabriel Druda. O compliance como "autorregulação regulada" e desafios técnicos de ordem prática. **Migalhas,** 9 abr. 2021. Disponível em https://www.migalhas.com.br/depeso/340170/o-compliance-como-autorregulacao-regulada. Acesso em: 01 jul. 2023.

[296] BARBAS, loc. cit.

também não é razoável entender que a sanção administrativa é suficiente para garantir o restabelecimento da paz pública e ordem social. Assim, havendo interesses difusos e coletivos, deveria haver direito intermediário, em que há ação, observados os princípios constitucionais, com provimento jurisdicional que traduziria a solução do conflito em imposição a pena, pois a ideia do direito de intervenção é ter processo com contraditório e ampla defesa, mas dentro de uma avaliação própria do direito administrativo, sem olvidar da prestação jurisdicional.

Isso é um modo de aprimorar as prementes necessidades evidenciadas, de modo a levar em conta também a celeridade pois quando se fala em tecnologias e sua constante alteração, métodos tradicionais podem não ser suficientes para tanto. Vê-se, portanto, que existe uma era de compliance digital, catalisados na questão de proteção de dados e privacidade – e aqui surge a questão dos dados sensíveis.

É fundamental buscar a conformidade por meio da utilização do compliance no ambiente da tecnologia digital. Tal cultura deve ser completamente promovida, especialmente neste período de transformação digital, quando a sociedade se depara com novas ferramentas tecnológicas que, devido à imprudência, falta de habilidade ou descuido, frequentemente acabam infringindo normas de proteção de dados. Como resultado, poderiam ocorrer danos às garantias, liberdades e direitos, por isso a necessidade de enfrentar tal realidade por meio de gestão preventiva, sempre focada nos direitos fundamentais e em mecanismos que incentivam a cibersegurança[297].

Fato é que as tecnologias e suas constantes mutações impactam diretamente na autorregulação de empresas transnacionais. Como ficará a metarrealidade/metaverso[298] e a utilização de IA em contexto no qual um robô pode "tomar decisão" baseado em um grupo de algoritmos, caracterizando conduta punida como delito (crime a honra, por exemplo)? Como será a avaliação da tomada de decisão? Quem alimentará o sistema para que tal comando seja

[297] LÓSSIO, Claudio Joel B. **Proteção de dados e compliance digital**. 2. ed. São Paulo: Almedina, 2023. *E-book*. p.107. ISBN 9786556279893. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556279893/. Acesso em: 01 nov. 2024.

[298] Nesse sentido, "metaverso é uma espécie de nova camada da realidade que integra os mundos real e virtual. Na prática, é um ambiente virtual imersivo construído por meio de diversas tecnologias, como Realidade Virtual, Realidade Aumentada e hologramas. Para visualizar o conceito, pense no filme Matrix, dirigido por Lilly e Lana Wachowski. No longa, as pessoas vivem em uma realidade virtual arquitetada por uma inteligência artificial assassina que usa seus corpos para produzir energia. O metaverso é mais ou menos por aí, mas sem as máquinas vilãs – pelo menos por ora. Nesse universo, que ainda não é real em sua totalidade, as pessoas poderiam interagir umas com as outras, trabalhar, estudar e ter uma vida social por meio de seus avatares (bonecos virtuais customizados) 3D. Ou seja, o objetivo é que pessoas que não sejam apenas observadores do virtual, mas façam parte dele". (INFOMONEY. Metaverso: tudo sobre o mundo virtual que está chamando a atenção dos investidores. **Infomoney,** 8 nov. 2022. Disponível em https://www.infomoney.com.br/guias/metaverso/. Acesso em: 1 nov. 2024.)

tomado? Como ficará a responsabilização da pessoa jurídica? São questões que demandam tempo e respostas que não podem ser tomadas de pronto.

Nesse sentido:

> Atingir o *Compliance* Digital, envolve tecnologia da informação e comunicação e o direito. Para atingir essa conformidade o caminho ocorre através das aplicações de padrões técnicos para que, por exemplo, a segurança da informação e uma reorganização da cultura corporativa seja atingida, pela determinação da governança e da execução da gestão.
> O *Compliance* Digital alberga na sua essência a função de alteração de técnicas, de processos, e da cultura organizacional através da sua própria reestruturação e das pessoas que o formam, envolvendo o Direito, a Gestão e Governança e a Tecnologia da Informação [...]
> A evolução das inovações fez e faz com que o ambiente mundial sofra transformações. Exemplo disso é o aparecimento do computador e da internet, que de certa forma são o berço tecnológico que deu origem ao ciberespaço [...]
> A relação entre pessoas tem vindo a sofrer revoluções devido aos avanços tecnológicos e ao surgimento de invenções que facilitam o quotidiano. O Direito, enquanto instrumento que regula a sociedade, não altera a essência das coisas podendo, então, os criadores adequar as suas invenções ou inovações aos princípios fundamentais, como o direito à privacidade, à proteção de dados, e à inviolabilidade das comunicações e correspondências, por exemplo. Para tal prática, são necessárias a procura e a aplicação do *Compliance* nesses novos produtos ou serviços[299].

Além disso, a IA está vinculada de uma forma muito forte a um binômio que precisa ser solucionado no que se refere à justiça: eficiência e construção de justiça. No âmbito de proteção de dados, isso intensifica a necessidade de adoção de critérios, especialmente no contexto internacional. Dessa forma:

> [...] nomeadamente algumas ISO da família 27000, como a 27001 e 27002. É igualmente primordial a execução da ISO 27701 e 29151 que trazem o *Compliance* digital para promover a proteção de dados de forma técnica e seguir a determinação jurídica presente no Regulamento Geral de Proteção de Dados da Europa. A ISO 27035 refere procedimentos direcionados ao âmbito forense e diretamente associados à Lei 46/2018, visto que são esses os procedimentos a ser seguidos pela equipe de resposta aos incidentes de fuga e violação de dados. No que visa a gestão do *Compliance* e antissuborno, podem serem elencadas as ISO 19600 e 37001, respectivamente.
> Os países não criam as suas próprias normas técnicas e, mesmo as normas internas – conforme acontece com a transposição de convenções internacionais -, podem ser trazidas para o seu ordenamento apenas de forma parcial. As normas técnicas são direcionadas, nesse caso, ao ambiente de segurança da informação e esse meio informático normalmente possui protocolos, tecnologias, sistemas idênticos no mundo todo. Como exceção, ocorre a hipótese de criação, pelo próprio Estado, de uma

[299] LÓSSIO, Claudio Joel B. **Proteção de dados e compliance digital**. 2. ed. São Paulo: Almedina, 2023. *E-book.* p.112. ISBN 9786556279893. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556279893/. Acesso em: 01 nov. 2024.

> tecnologia que se utilize dentro das suas fronteiras, de forma exclusiva, e em nada impedindo a utilização da ISO como base para normas internas, como a NBR[300].

Ainda em relação as ISO:

> [...] diante do Direito e de um ordenamento jurídico, é necessário entender o que são as *softlaws*. O instrumento que regula a sociedade é o Direito e, quando essa regulação está direcionada ao contexto mundial, elenca-se o Direito Internacional [...] O ambiente internacional possui diversas normas, como declarações, acordos, convenções, tratados, e ainda normas de padrão técnico internacional. A *Softlaw* pode ser considerada um padrão de norma flexível não positivada na ordem jurídica do país, pelo que pode ser elencada a ISO 27701 e 28151. Esta norma, não sendo obrigatória, constitui a essência para se a atingir o *Compliance* de um diploma jurídico, como o Regulamento Geral de Proteção de Dados da Europa.
> [...]
> A aplicação de *softlaws* como a ISO 27701, que é um marco regulatório internacional não obrigatório, torna-se necessária no âmbito de empresas públicas ou privadas. Está-se, deste modo, a procurar a sua adequação diante do Regulamento Geral de Proteção de Dados da Europa e, por consequência, de outros diplomas de proteção de dados de diferentes Estados. Trata-se, indubitavelmente, de um marco para o *Compliance* Digital.
> Mas como implementar uma ISO? Primeiramente é necessário estudar detalhadamente a ISO em questão, para compreender quais os controles que são determinados por ela. Assim, através de uma auditoria na organização que se deseja implementar a ISO, é comparado quais controles da ISO já estão implementados, quais controles não estão implementados e quais precisam melhorar[301].

O avanço tecnológico provoca alterações nos hábitos sociais. Hoje, diante da era da informação, numa época em que todos os dados (e a forma de tratamento) evoluem rapidamente, o que gera necessidade de normas regulatórias para essa conformidade digital.

Noutro giro, hoje, a empresa é a própria consumidora dos serviços de implementação da LGPD, representando recursos financeiros, tempo e comprometimento com direitos. Trata-se de processo de compliance abrangente e sensível, exigindo elevado grau de detalhamento e colaboração de especialistas de diversas disciplinas[302].

Além disso, hoje, vincular-se a ações de interesses de tutela de direitos difusos e coletivos, muitas vezes pode levar à eficiência, mas afastada do sentido de justiça. Atualmente, tem-se o Direito Penal supraindividual, notadamente diante dos avanços tecnológicos. Conforme elucida Claudia Cristina Barrilari:

> [...] as objeções ao bem jurídico supraindividual giram em torno das dúvidas quanto à sua compatibilidade com a tutela penal própria de um Estado democrático e,

---

[300] LÓSSIO, Claudio Joel B. **Proteção de dados e compliance digital**. 2nd ed. São Paulo: Almedina, 2023. *E-book*. p.132. ISBN 9786556279893. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556279893/. Acesso em: 01 nov. 2024.
[301] Ibid., p.133.
[302] Ibid., p.147.

> consequentemente, vinculada à reserva da *ultima ratio*. Há que se optar por determinado pressuposto que legitime a tutela desses bens e que, ao mesmo tempo, seja compatível com a evolução da sociedade moderna e, consequentemente, admita a proteção penal de bens cuja defesa seja imanente para a sociedade. Corrobora, ainda, o fato de a tutela do bem coletivo, desde a origem da teoria do bem jurídico, vir atrelada ao objetivo de satisfazer uma necessidade da sociedade, pois a proteção do bem individual figura insubsistente.
> De fato, na formação histórica da teoria do crime, desde o período anterior ao Iluminismo, era o delito concebido como violação de um dever do indivíduo com o Estado. Desse modo, o único fator legitimante do crime era a vontade do detentor do poder. Para que se retirasse o poder do Estado na definição do ilícito surgiu o conceito de lesão a direito subjetivo. Com isso, a essência do delito passa a necessidade de uma lesão a um interesse individual cuja consequência será a verificação de um dano social. Ocorre que a definição de delito como lesão a direito subjetivo, e, portanto, relacionada a direitos individuais, passa a ser insuficiente para acobertar crimes que não se relacionavam a direitos individuais, como os delitos religiosos e contra o Estado.
> [...] A análise histórica do conceito de bem jurídico acaba por mostrar que já na sua origem não se continha nos estreitos limites do bem jurídico individual. É possível afirmar que o Direito Penal deve acompanhar a evolução da sociedade e, para tanto, estabelecer uma política criminal de proteção de bens jurídicos coletivos. A tutela penal dos interesses difusos deriva de uma exigência política de satisfação de necessidades essenciais concretas. Ao que se alia a ideia de autonomia dos bens supraindividuais[303].

Dentro dessa questão supraindividual, verifica-se cada vez mais a necessidade de um espaço internacional próprio, para realizar o debate e apontar alternativas para tanto.

A coletividade, de maneira geral, possui interesses ligados às práticas de conformidade. A sociedade da informação é fundamentalmente relacionada à economia, representando uma sociedade voltada para o capital. Dessa forma, a autorregulação supervisionada favorece o participante que adota práticas de concorrência justas e padrões éticos no ambiente empresarial, gerando benefícios para todos[304].

Acerca da autorregulação, José Leite Guimarães explica que:

> Na globalização, a produção de normas não é mais exclusiva do Poder Público, surgindo normas de controle que mais se adequam à nova ordem econômica mundial emanadas pela própria sociedade. A regulamentação imposta pelo Estado ao cidadão não é capaz de controlar o bom funcionamento das instâncias empresariais e a ordem econômica, surgindo assim a autorregulação.
> O Estado precisou ser recriado, não podendo ser mais um comando hierárquico e verticalizado; ele precisa ser um Estado que esteja entrelaçado com a sociedade de uma forma horizontal, podendo dessa maneira se integrar de forma mais maleável à sociedade e aos atores da ordem econômica.
> [...]
> Na sociedade moderna ou na sociedade de risco, muitos são os "sistemas sociais funcionais", sendo um deles os grandes núcleos empresariais, e essa diversidade e o aumento do conhecimento geral também o implemento do risco. Se o Estado for o único responsável pela manutenção dessa engrenagem, viveremos a situação em que a edição de normas poderá ser imprecisa ou tardia. A sociedade pode sofrer uma

[303] BARRILARI, Claudia Cristina. **Crime empresarial, autorregulação e compliance.** 2. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 39-40.
[304] SANTOS, Fábio Antônio Tavares dos. **Direito Penal Empresarial** – a responsabilidade penal horizontal**.** São Paulo: LiberArs, 2022, p. 49.

> verdadeira lacuna regulatória, que, com a autorregulação e sua dinâmica mais atualizada à sociedade de risco, poderá suprir esse vácuo com a edição de normas devidamente baseadas nas tecnologias existentes e elaboradas por quem gera e assume o risco e que serão responsabilizados por sua inobservância.
> O crescimento da autorregulação pode ser sentido nos mais diversos segmentos, inclusive nos negócios globalizados, onde por vezes a legislação pátria não poderia ser aplicada, ficando a atividade econômica carente de normas que pudessem ser aplicadas na sua gestão [...][305].

Noutro ponto, os conceitos de governança corporativa como sendo conjunto de práticas e políticas institucionais para regular e orientar o funcionamento de empresa. O fim objetivado sempre será a garantia de ética e integridade, notadamente para prevenção à lavagem de dinheiro. Aqui, a empresa, desde o início, analisa os riscos, sem olvidar de todas as questões dos dados digitais de que, inevitavelmente, trata no próprio âmbito de seu escopo.

A empresa, portanto, assume um papel garantidor, sendo que os gestores têm a responsabilidade de prevenir a materialidade dos riscos que originalmente aceitaram. Desse modo, os programas de compliance devem ter, acima de tudo, dever informacional para promover simetria e clareza na atuação[306].

Nesse sentido, alguns questionamentos surgem:

> Se for possível a otimização dessa integração, é de pensar que as empresas poderão manejar o padrão autorregulatório de modo a alinhá-lo com as expectativas normativas de cada Estado. É nesse contexto que a tutela estatal será mais flexível ou mais rígida, de acordo com o grau de estabilidade social, e, evidentemente, as empresas não podem ter seus mecanismos autorregulatórios rigidamente fixados. Se a estabilidade social for débil, a tutela estatal poderá variar em duas direções: na primeira, pode ser fraca, própria de Estados onde se destaca uma fragilidade política e institucional. É o que ocorre nas nações com acentuado grau de corrupção em todas as esferas, sem leis efetivas ou em que a lei, apesar de existente, é ineficaz. Nesse primeiro cenário, como se autorregula uma corporação que tenha negócios nesse Estado?
> No segundo caso, é possível que o Estado esteja orientado para o fortalecimento de sua tutela estatal. Isso pode se dar por força das exigências das normativas de *soft law* [...] ou, ainda, para atender às necessidades do mercado ou aos interesses políticos. Estar-se-ia, nesse caso, diante de uma estabilidade social fraca e de uma tutela estatal coercitiva. Nesse cenário, como se autorregulará uma corporação?
> Mudando o foco para os interesses da corporação, pode-se também questionar qual tutela estatal será mais adequada para sancionar ou fiscalizar a empresa.
> Evidentemente, essas são questões para as quais não há respostas uníssonas. Contudo, é de se pender em conciliar os interesses distintos que agora se apresentam de modo a estruturar as relações entre as corporações e Estado para atender aos interesses da empresa e aos interesses públicos e sociais. Por esses motivos, a interação entre governança e corporativa, responsabilidade social da empresa e autorregulação pode servir não somente aos objetivos específicos de cada um desses mecanismos como,

---

[305] GUIMARÃES, José Leite Júnior. **Responsabilidade Penal das pessoas jurídicas nos crimes econômicos –** Sociedade de risco e empresa. São Paulo: Dialética, 2023, p. 14-15.
[306] FILARDI, Rosemaria Adalardo; SOUZA, Damares Pereira de. Programas de compliance como autorregulação. **DIGE – Direito Internacional e Globalização Econômica,** v. 2 n. 02, p. 46-59, 2023. Disponível em: https://revistas.pucsp.br/index.php/DIGE/article/view/64290. Acesso em: 08 ago. 2024, p. 53-54.

> também, a constituir conjugadamente um novo e importante elemento de prevenção de ilícitos corporativos[307].

Não se pretende esgotar o tema que, aliás, ainda é relativamente novo. Diversos pontos devem ser levados em consideração, especialmente quanto ao aumento de dados digitais. É possível afirmar que chegará um momento em que a quantidade de conteúdo armazenado será tão acentuada que o próprio alimentador desenvolverá um trabalho de estabelecer elementos, mas as decisões tomadas pelo robô (já tratando-se aqui da questão de IA) levarão em conta não só os dados presentes, mas também pretéritos e o problema é que, ao trabalhar com o compliance, existem questões de natureza ética e social.

Em suma, dentro da linha de atividade de empresa existe uma série de decisões que serão tomadas pelo corpo executivo e, com o passar do tempo, passarão a ser adotadas pelos robôs. A principal discussão é: como não responsabilizar aqueles do corpo diretivo ou o próprio corpo em si, pela prática de atividades vinculadas por sua linha de atuação, mas que foram tomadas por máquinas em razão dos elementos e da essência dos dados que lhe foram fornecidos? Outras discussões surgem, por exemplo, se essas ferramentas serão suficientes para a análise dos dados e como ficará, de todo modo, sua proteção?

Por derradeiro e dentro desse contexto, foi apresentado o PL 2338/2023, estabelecendo normas gerais de caráter nacional para o desenvolvimento e uso responsável de sistemas de IA no Brasil, em consonância com os termos da LGPD. Tudo isso impacta compliance e os profissionais, sendo fundamental a atualização constante.

A questão é ainda mais polêmica quando se trata de empresa transnacional e proteção aos direitos humanos, pois é necessário trabalhar também com a ideia de jurisdição internacional, pois não se pode crer que cada Estado irá satisfazer a todas as questões, notadamente porque existe a questão do poder econômico, afinal, necessitam também de investimentos.

4.3 LAVAGEM DE DINHEIRO: PERSPECTIVAS NO COMBATE AO CRIME ECONÔMICO

As raízes contemporâneas do fenômeno da lavagem de dinheiro têm início com a criminalização do tráfico de drogas e da venda de bebidas alcoólicas nos Estados Unidos, entre

---

[307] BARRILARI, Claudia Cristina. **Crime empresarial, autorregulação e compliance.** 2. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 89-90.

1920 e 1933, devido à proibição, à época, de fabricação, comercialização, transporte, importação e exportação. Assim, os comerciantes se uniram e passaram a operar de maneira ilegal, obtendo lucros consideráveis que, contudo, não poderiam ser exibidos de forma clara, vez que não havia justificativa formal para tanto[308].

À época, Al Capone e outros empregavam, entre as práticas, o uso de lavanderias, que permitiam combinar ativos legais e ilegais, visando justificar a origem dos recursos financeiros, uma das razões para o termo "*money laundering*"[309].

Em suma, lavagem de dinheiro consiste no processo "por meio do qual se opera a transformação de recursos obtidos de forma ilícita em ativos com aparente origem legal, inserindo, assim, um grande volume de fundos nos mais diversos setores da economia"[310].

No Brasil, é tipificada como crime pelo artigo 1º da Lei 9.613/98:

> Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.
> Pena: reclusão, de 3 (três) a 10 (dez) anos, e multa.
> § 1º Incorre na mesma pena quem, para ocultar ou dissimular a utilização de bens, direitos ou valores provenientes de infração penal:
> I - os converte em ativos lícitos;
> II - os adquire, recebe, troca, negocia, dá ou recebe em garantia, guarda, tem em depósito, movimenta ou transfere;
> III - importa ou exporta bens com valores não correspondentes aos verdadeiros.
> § 2º Incorre, ainda, na mesma pena quem:
> I - utiliza, na atividade econômica ou financeira, bens, direitos ou valores provenientes de infração penal;
> II - participa de grupo, associação ou escritório tendo conhecimento de que sua atividade principal ou secundária é dirigida à prática de crimes previstos nesta Lei.

E, sendo atividade complexa, envolve etapas, quais sejam, colocação, ocultação e integração. A primeira, que é a colocação dos recursos ilícitos no sistema econômico (*placement*), busca distanciar os recursos de sua origem, com o fim de dificultar a identificação da procedência. Dessa forma:

> [...] valores podem ser introduzidos nos bancos por meio de depósitos feitos por diversas pessoas em várias contas, em pequenas quantias, em determinado período de tempo e que, individualmente, não geram suspeitas. Essa técnica é conhecida como smurfing e seu objetivo é driblar o controle dos bancos ao fragmentar os valores depositados a fim de não alcançar o valor que obrigatoriamente deveria ser comunicado às autoridades. Nesta fase, também é utilizada a técnica de misturar recursos ilícitos, originados por alguma atividade legítima, com os ilícitos, sem a

[308] ARAS, Vladimir; LUZ, Ilana M. **Lavagem de dinheiro:** comentários à Lei n. 9.613/1998**. São** Paulo: Almedina, 2023. *E-book.* p. 23. ISBN 9786556279152. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556279152/. Acesso em: 01 nov. 2024.
[309] ARAS, loc. cit.
[310] CAPEZ, Fernando. **Legislação Penal Especial.** 18. ed. São Paulo: Saraivajur, 2023, p. 527.

> possibilidade de descobrir os recursos que são ilegais, uma vez que o dinheiro em espécie não apresenta "carimbos", que atestem sua origem. A técnica chama-se commingling ou mescla. Outras formas podem ser: conversão dos recursos ilícitos em moeda estrangeira, compra de instrumentos negociáveis, compra de bens imóveis, obras de arte, entre outras[311].

A segunda (*layering*) é a ocultação por meio de camuflagem, ou seja, há a dissimulação, uma série de negócios e movimentações com o fim de dificultar ou impedir o rastreamento, com o objetivo de quebrar a cadeia de evidências, tornando mais difícil a investigação. Essa etapa pode incluir a transformação de dinheiro depositado em ativos financeiros como títulos e ações, por exemplo, e a aplicação em propriedades e empreendimentos[312].

Por fim, a integração (*integration),* que é a fase final, com incorporação formal, ou seja, os recursos ilícitos são de fato inseridos no sistema financeiro, com aspecto de legalidade:

> As organizações criminosas investem em empreendimentos que facilitem suas atividades, utilizando-se da cadeia da ilegalidade para se ajudarem mutuamente. Vendem bens, sejam eles imóveis ou obras de arte, adquiridos com o dinheiro ilícito a preços abaixo de mercado, pelo preço cheio ou superfaturado, lavando uma boa quantidade do dinheiro. É muito comum que essas transações sejam realizadas utilizando-se de "laranjas" para manter o contraventor no anonimato[313].

A finalidade, portanto, é sempre dificultar a identificação da origem criminosa dos recursos, utilizando técnicas como transferências internacionais. Tudo isso, dentro de um contexto de prova, se revela importante objeto de estudo, afinal, combater o crime organizado traz nuances variadas[314].

Para além da análise da legislação em vigor, fato é que a lavagem de capitais ganha novos contornos com a internet, a exemplo de uso de criptoativos e outras moedas digitais, havendo sofisticação no modo como ocorre. Nesse sentido:

> [...] a maior facilidade de interação à distância com a difusão das telecomunicações e da internet, a maior disponibilidade e rapidez de meios de transporte de bens por todo o globo e a eliminação de barreiras domésticas à livre circulação de pessoas, mercadorias, serviços e valores são fatores que não foram ignorados pelos operadores de atividades ilícitas, com o fim de adquirir, transportar e distribuir drogas, mercadorias contrafeitas, armas e munições e praticar os mais variados crimes, como o tráfico humano e a corrupção. O quadro logístico montado para atender a legítimos negócios do comércio exterior passou a ser utilizado por organizações criminosas em

---

311 RIZZO, Maria Balbina M. **Prevenção da lavagem de dinheiro nas organizações**. 2. ed. São Paulo: Trevisan Editora, 2016. *E-book.* p. 24. ISBN 9788599519875. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788599519875/. Acesso em: 01 nov. 2024.
312 Ibid., p. 25.
313 RIZZO, loc. cit.
314 Para o STF as três fases não precisam ocorrer para configurar a lavagem de capitais, ou seja, basta uma delas, de forma alternativa, para a caracterização do delito (AP 470/MG – Info 679).

> todo o mundo e também por lavadores de capitais ordinários. As vantagens econômicas advindas desses negócios ilícitos passaram a transitar pela economia global, contando com as mesmas facilidades dos capitais legítimos, dada a importância da livre circulação de capitais em espaços integrados[315].

Ainda:

> A globalização impulsionou a evolução desse ato eliminando totalmente seu caráter local, embora no Brasil um grande volume dos recursos ilicitamente gerados seja lavado localmente. A lavagem de dinheiro tem fluxo contínuo, funciona ininterruptamente 24 horas por conta dos fusos horários, ou seja, quando um centro financeiro fecha os negócios, outro se abre para iniciá-los.
> A velocidade e a eficiência dos sistemas eletrônicos de transferências internacionais de fundos, por exemplo, também beneficiam os criminosos na etapa de ocultar a origem dos recursos.
> No mundo todo são movimentadas diariamente cerca de 17 milhões de transferências eletrônicas de fundos, segundo informações do Society for Worldwilde Interbank Financial Telecommunication/Sistema Mundial de Comunicações Interbancárias (SWIFT), que é a plataforma por meio da qual são processadas as transferências internacionais. É nesse veloz mundo tecnológico que também proliferam as transferências de recursos ilegais camufladas pelo assombroso volume diário.
> As organizações criminosas não respeitam fronteiras e expandem suas atividades para aqueles mercados que melhor se prestem ao seu negócio; escolhem países com sistemas de controle e fiscalização mais brandos e maior flexibilidade das leis e menor rigidez na adoção de políticas globais de cooperação internacional[316].

As metamorfoses criminais são tão evidenciadas que a Lei n. 9.613/98 passou por diversas alterações. Dentre elas, destaca-se a Lei n. 13.974/2020, que regulou as competências do Conselho de Controle de Atividades Financeiras (Coaf), que é a Unidade de Inteligência Financeira (UIF), órgão de inteligência que atua, principalmente, na prevenção e combate à lavagem de dinheiro, no entanto, sendo órgão de controle, daí porque o fornecimento de quaisquer dados e informações com finalidade de investigação criminal deve observar o devido processo legal[317].

Nesse sentido, a Lei de Lavagem de Dinheiro determina que as instituições financeiras e demais pessoas físicas e jurídicas que trabalhem com recursos financeiros, por exemplo, comuniquem ao Coaf/UIF qualquer movimentação que seja considerada "atípica" (art. 11). Trata-se aqui de importante mecanismo de prevenção já que é por meio da lavagem de dinheiro

---

[315] ARAS, Vladimir; LUZ, Ilana M. **Lavagem de dinheiro: comentários à Lei n. 9.613/1998**. São Paulo: Almedina, 2023. *E-book*. p.23. ISBN 9786556279152. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556279152/. Acesso em: 01 nov. 2024.
[316] RIZZO, Maria Balbina M. **Prevenção da lavagem de dinheiro nas organizações - 2ª Edição**. 2nd ed. São Paulo: Trevisan Editora, 2016. *E-book*. p. 23-24. ISBN 9788599519875. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788599519875/. Acesso em: 01 nov. 2024.
[317] MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 134.

que diversos outros crimes (graves) são cometidos. Nesse sentido, o STF entendeu que é possível o compartilhamento dos relatórios com os órgãos de persecução penal para fins criminais, sem a obrigatoriedade de prévia autorização judicial, diante da natureza de peças de informações (RE 1055941/SP, Rel. Min. Dias Toffoli, julgado em 4/12/2019 – tema 990).

Aliás, consta no Manual de Cooperação Jurídica Internacional:

> Diante da realidade atual, consubstanciada na quase total inexistência de limites fronteiriços para a prática criminosa, bem como considerando a crescente ampliação da delinquência transnacional, as autoridades estatais responsáveis pela condução de investigações criminais, pela persecução e pelo julgamento de processos penais começaram a perceber o consequente aumento da necessidade de obtenção de diligências e elementos probatórios no exterior, a fim de colaborar com a elucidação da autoria e materialidade de determinada conduta criminosa e com a apuração da verdade real dos fatos.
> Apesar de os países constantemente se preocuparem em manter, resguardar, fiscalizar e monitorar seus limites territoriais, até por conta do fato de que o território físico, terrestre ou marítimo, consiste em um elemento imprescindível à própria condição de Estado soberano, tal atitude não consegue impedir, na maioria das vezes, que a criminalidade existente dentro no meio social seja perpetrada mediante condutas ilícitas que transpassem suas fronteiras naturais.
> [...]
> Não é demais salientar que essa realidade é fomentada em grande parte pela ineficiência e lentidão dos controles estatais sobre diversos fenômenos inerentes à evolução da sociedade e que vêm influenciando profundamente a comunidade internacional nas últimas décadas – tais como, a globalização da economia, a facilidade de comunicação e de troca de informações, o incremento da rede mundial de computadores, a agilidade na realização de operações financeiras, o aumento do comércio exterior e também o aumento das possibilidades das pessoas realizarem viagens internacionais.
> [...]
> Nesse contexto, cresce em importância a cooperação jurídica internacional em matéria penal – como mecanismo eficaz de auxílio jurídico entre os Estados, apto para colaborar com o combate ao crime, com a recuperação de ativos ilícitos e com a apuração da verdade dos fatos sobre determinada prática delituosa que contenha algum elemento transnacional – cujo conhecimento e correta utilização faz-se imprescindível nos tempos atuais, sob pena de frustração da aplicação da lei e da realização da própria justiça criminal[318].

Assim sendo, é imperativa a necessidade de aprimoramento do sistema de controle das instituições financeiras, não com exigências maiores ou fiscalizações implacáveis, mas por meio da correta escolha dos agentes de controle, em função de sua missão constitucional.

Aqui, fala-se em macrocriminalidade econômica. Não se pretende aqui fazer uma análise de todo o conceito pertinente à lavagem de dinheiro, mas entender a problemática atual e como as ferramentas de investigação (digital) podem auxiliar nesse sentido.

---

[318] BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. **Manual de Cooperação Jurídica Internacional: Matéria Penal e Recuperação de Ativos**. 4. ed., 2019. Disponível em https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagem-de-dinheiro/drci/publicacoes/manuais/cooperacao-juridica-internacional-em-materia-penal/manual-penal-online-final-2.pdf. Acesso em: 11 jul. 2024.

Por conseguinte, não se pode deixar de observar o problema contemporâneo e real quanto à ampla divulgação de plataformas de jogos digitais por meio de redes sociais.

No ordenamento jurídico brasileiro, a regulamentação dos jogos de azar é estabelecida pela Lei das Contravenções Penais (Decreto-Lei n. 3.688/1941[319]). Ocorre que em dezembro de 2018 foi aprovada a Lei n. 13.756, que passou a autorizar a exploração comercial de apostas esportivas no Brasil, apenas em relação a loteria e apostas de quota fixa. Ainda, a Lei 14.790/2024 passou a exigir que as empresas tenham endereço no Brasil, definindo tributação e jogos on-line.

Permanece, portanto, um limbo, que é justamente a questão das empresas de apostas on-line que, a despeito de operarem no Brasil, possuem sua base em território estrangeiro, hospedadas em sua maioria em plataformas clandestinas e não auditáveis. Assim, o que se vê é o aumento de apostas, com o mercado sendo efetivamente atingido, sem que haja regulamentação correta. Abre-se, portanto, porta para ilegalidades como a lavagem de dinheiro, por exemplo.

A questão da regulamentação vai além: sem norma regulatória há prejuízo na receita em âmbito nacional. O mercado fica defasado, podendo haver inflação, queda nas taxas de crescimento e investimento, acréscimo de juros, entre outros, que podem ocasionar prejuízos irrecuperáveis para a própria economia.

Mais do que isso: o regulamento correto protegerá o próprio consumidor que, hoje, se vê em situações nas quais nem sequer sabe se irá receber aquele dinheiro que foi colocado na aposta.

Observa-se, diariamente, que a polícia judiciária vem deflagrando operações, mas é certo que o caminho para a regulamentação caminha a passos lentos, gerando problemas.

---

[319] Art. 50. Estabelecer ou explorar jogo de azar em lugar público ou acessível ao público, mediante o pagamento de entrada ou sem ele: Pena – prisão simples, de três meses a um ano, e multa, de dois a quinze contos de réis, estendendo-se os efeitos da condenação à perda dos moveis e objetos de decoração do local. § 1º A pena é aumentada de um terço, se existe entre os empregados ou participa do jogo pessoa menor de dezoito anos. § 2º Incorre na pena de multa, de R$ 2.000,00 (dois mil reais) a R$ 200.000,00 (duzentos mil reais), quem é encontrado a participar do jogo, ainda que pela internet ou por qualquer outro meio de comunicação, como ponteiro ou apostador. § 3º Consideram-se, jogos de azar: a) o jogo em que o ganho e a perda dependem exclusiva ou principalmente da sorte; b) as apostas sobre corrida de cavalos fora de hipódromo ou de local onde sejam autorizadas; c) as apostas sobre qualquer outra competição esportiva. § 4º Equiparam-se, para os efeitos penais, a lugar acessível ao público: a) a casa particular em que se realizam jogos de azar, quando deles habitualmente participam pessoas que não sejam da família de quem a ocupa; b) o hotel ou casa de habitação coletiva, a cujos hóspedes e moradores se proporciona jogo de azar; c) a sede ou dependência de sociedade ou associação, em que se realiza jogo de azar; d) o estabelecimento destinado à exploração de jogo de azar, ainda que se dissimule esse destino.

De todo modo, fica evidente o caminho digital traçado pelo delito de lavagem de dinheiro, seja em aplicativos, mensagens ou dispositivos criptografados, além, claro, do próprio armazenamento em nuvem (*cloud*).

Novamente se vê a necessidade de observar estritamente a cadeia de custódia, conferindo validade e confiabilidade a tais provas.

Nesse sentido, a própria lei prevê a possibilidade de quebra de sigilo bancário e fiscal (art. 17-B da Lei n. 9.613/98[320]). O STF, na ADI 4.906/DF, julgado em 11/9/2024 (info 1150), de relatoria do Min. Nunes Marques, entendeu que é constitucional referida norma:

> AÇÃO DIRETA DE INCONSTITUCIONALIDADE. LEI N. 9.613/1998, ART. 17-B. COMPARTILHAMENTO DE DADOS CADASTRAIS COM ÓRGÃOS DE PERSECUÇÃO CRIMINAL. DESNECESSIDADE DE AUTORIZAÇÃO JUDICIAL. 1. A Associação Brasileira de Concessionárias de Serviço Telefônico Fixo Comutado (Abrafix) não tem legitimidade para impugnar inteiro teor de dispositivo quando impactadas entidades por ela não representadas. Preliminar da Advocacia-Geral da União acolhida, conhecendo-se parcialmente da ação, somente no que diz respeito à expressão "empresas telefônicas". 2. Conforme entendimento do Supremo, a proteção versada no art. 5º, XII, da Constituição Federal refere-se à comunicação de dados, e não aos dados em si mesmos. 3. O direito à privacidade, entre os instrumentos de tutela jurisdicional, se consubstancia no sigilo, que consiste na faculdade de resistir ao devassamento de informações cujo acesso e divulgação podem ocasionar dano irreparável à integridade moral do indivíduo. O acesso ao conteúdo de certos objetos é medida excepcional que depende de autorização judicial e somente se justifica para efeito de investigação criminal ou instrução processual penal. 4. O objeto de tutela mediante a imposição de sigilo não alcança os dados cadastrais. Isso não significa que essas informações dispensem tutela jurisdicional, mas apenas que a tutela em virtude do direito à privacidade não se concretiza via sigilo. 5. O direito fundamental à proteção de dados e à autodeterminação informativa (CF, art. 5º, LXXIX) impõe a adoção de mecanismos capazes de assegurar a proteção e a segurança dos dados pessoais manipulados pelo poder público e por terceiros. 6. É compatível com a Constituição de 1988 o compartilhamento direto de dados cadastrais genéricos com os órgãos de persecução penal, para fins de investigação criminal, mesmo sem autorização da Justiça. 7. Ação direta de inconstitucionalidade de que se conhece em parte, e, nessa extensão, pedido julgado improcedente[321].

A questão retorna àquilo que já se viu sobre privacidade e os direitos de personalidade contra interferências indevidas na vida pessoal. Contudo, dados cadastrais como nome, endereço e filiação são informações objetivas, fornecidas pelo indivíduo, não acobertadas pelo sigilo. Em suma, não interferem diretamente na questão da personalidade.

---

[320] Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

[321] BRASIL. Supremo Tribunal Federal. **ADI 4.906/DF**, Rel. Min. Nunes Marques, Tribunal Pleno, julgado em 11/09/2024, publicado em: DJe-s/n, 24/10/2024. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%204906%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em: 07 out. 2024.

Portanto, diante da ausência de regulamentação, a jurisprudência vem se debruçando sobre o tema, tratando de casos concretos. Mas é certo que a cada dia, novas questões serão postas à prova, demandando que o ordenamento jurídico esteja integrado.

A falha na colheita culmina na quebra da cadeia de custódia e em ineficácia do direito.

As apostas movimentam milhões de reais, e esse aumento traz consigo a preocupação quanto às práticas criminosas que circundam as operações, notadamente a lavagem de capitais.

Alguns questionamentos devem ser feitos: qual o impacto na vida dos brasileiros (diante do evidente aumento de dívidas geradas por tais aplicativos)? Qual o impacto na economia? Como poderia haver o monitoramento dessas atividades, sem interferir na própria proteção dos dados pessoais?

É fato: o crescente acesso às plataformas on-line facilita o fluxo de grandes quantias, sem nenhum controle.

Os crimes macroeconômicos são capazes de atingir toda a coletividade ou um determinado grupo social, ou seja, quase sempre acontece em grande escala, estando relacionados a crimes que ocorrem nos moldes empresariais e que possuem, fundamentalmente, cunho econômico, sendo difícil delimitar onde eles começam e terminam.

A questão que novamente se traz é: seria possível falar em relativização das garantias constitucionais no combate à macrocriminalidade econômica? Sem esgotar o tema, em um primeiro momento pode-se dizer que as garantias constitucionais podem ser relativizadas em favor da sociedade, sem, no entanto, restringir os direitos dos acusados.

O regramento jurídico trazido pela CF/88 dispôs que tanto as normas definidoras dos direitos fundamentais quanto as garantias visam preservar a individualidade e a coletividade. Assim, percebe-se que, mesmo em se tratando de regras, existe a ponderação de princípios valorativos do Estado Democrático de Direito em algumas situações.

Em casos de conflitos entre eles, para que se chegue a um consenso, faz-se necessário que um dos lados cedam ou que ambos cedam em partes. O mesmo ocorre quando há um embate principiológico, o que não significa que eles são inválidos, no entanto, deve ser levada em consideração a importância de determinado princípio na situação em questão, tendo em vista que um pode pesar mais do que o outro.

Cabe ao Estado analisar quais casos poderão interferir na esfera individual ou coletiva para aplicar o que versa o princípio da proporcionalidade. Para comprovar se a norma é restrita de direitos e garantias fundamentais, deve ser observado se ela, em seu alcance, afeta conteúdos relacionados aos direitos fundamentais. Desse modo, será necessário determinar os limites, bem

como o âmbito protetivo de direito que será flexibilizado, sua finalidade, qual a natureza da restrição, o tipo e os limites que a Constituição estabelece.

Dessa forma, ressalta-se a relevância de uma abordagem constitucional penal distinta que favoreça a investigação de crimes macroeconômicos, os quais se tornam progressivamente mais complexos. Essa evolução torna o trabalho das forças policiais responsáveis pelas investigações e do sistema judiciário igualmente mais desafiador ao aprofundar-se na apuração dos fatos, visando avaliar a conduta e a responsabilidade do acusado durante o decorrer do processo. É evidente que há uma preocupação especial em todas as etapas, buscando resguardar os direitos e as garantias individuais do investigado.

Essa situação demonstra que tanto o direito penal como o direito processual penal não dão conta de tratar com a devida eficiência essa modalidade de crime, pois ainda faz uso dos mesmos instrumentos jurídicos para toda ordem social, que, pela sua natureza, tem a complexidade inerente a ela.

O Estado, diante de uma sistemática processual penal ultrapassada, destaca a necessidade de se reestruturar para lidar com a macrocriminalidade, buscando respostas condizentes com as ameaças que estas práticas representam para a sociedade. Isso se deve ao fato de que esses crimes possuem um alcance significativo, afetando tanto as vítimas quanto os danos, sejam eles individuais ou coletivos. Permanecer inerte representa o risco de frustrar uma das funções essenciais do Estado, que é prevenir conflitos, garantindo a paz e protegendo os bens jurídicos relevantes.

A alteração do sistema legal se faz essencial diante das frequentes mudanças sociais que ocasionam, por sua vez, o aparecimento de delitos que a legislação deve reconhecer e proteger, além de buscar métodos mais ágeis e eficazes para enfrentá-los.

O principal obstáculo da ordem jurídica reside em equilibrar o confronto entre os interesses do Estado e os direitos dos indivíduos durante a fase de coleta de evidências em casos de crimes financeiros. Esses aspectos se conectam diretamente aos objetivos centrais do sistema penal, que visam salvaguardar os direitos fundamentais e assegurar a realização da justiça penal de maneira eficaz.

Dessa maneira, o Direito Penal necessita de uma interpretação mais ampla de suas finalidades, devendo não apenas impor punições como uma obrigação do Estado, mas também assegurar um ambiente de segurança.

É inegável que o Estado não deve ultrapassar seus limites no poder de punir, necessitando de fundamentos excepcionais para limitar, quando necessário, as garantias

individuais. No entanto, é indiscutível a seriedade dos delitos financeiros, de modo que essa justificativa deve estar incorporada nas iniciativas governamentais de enfrentamento.

5 FORNECIMENTO DE DADOS POR EMPRESA TRANSNACIONAL: ACORDOS DE COOPERAÇÃO INTERNACIONAL *VERSUS* SOBERANIA NACIONAL

5.1 CONFLITOS DE JURISDIÇÃO

A natureza descentralizada da internet dificulta a possibilidade de identificação do responsável pelo conteúdo que circula nesse espaço. Nesse sentido, a transdisciplinariedade entre os acordos internacionais e a soberania nacional deve ser analisada de forma crítica, especialmente diante da necessidade de regulação quanto à responsabilidade das empresas transnacionais, com ênfase à tutela anômala destinada à culpabilidade empresarial e dos desafios decorrentes de sua aplicação.

E, se de um lado a facilitação do domínio digital se revela ser de grande importância, de outra tenciona a necessidade de maior vigilância, já que haverá maior probabilidade de serem difundidos diversos conteúdos – criminosos – e, como consequência, surgem dúvidas acerca da competência para dirimir conflitos[322].

Dessa forma, é notório que o direito, frente à globalização dos mercados mostra-se, na sociedade internacional atual, claramente inadequado aos novos paradigmas. Tal fato clama, assim, intervenção de novas disciplinas nesse sentido.

Contudo, observa-se a ausência de universalidade do processo, o que pode culminar em inobservância de direitos conquistados ao longo do tempo. Cingindo-se o Estado, em ação generalizada e abstrata, em estabelecer normatizações como efeito intimidador e preventivo aos que desafiem violação às normas já consagradas.

Conflitos que envolvem informações pessoais e empresas, como o Facebook, que possui sede nos Estados Unidos, estarão sujeitos a aspectos do Direito Internacional Privado, o que definirá a jurisdição apropriada e a legislação que será aplicada[323].

Independentemente do tipo de dado mencionado - seja ele genérico, metadados ou informações pessoais - todos podem ser transferidos e armazenados em bases de dados. A movimentação de dados pode acontecer entre servidores situados em diferentes países, estando, assim, sujeitos a diversas legislações[324].

---

[322] CASTRO, E. L. de F.; WINTER, P. P. O conflito de jurisdições em caso de violação de direitos da personalidade por publicação na internet. **Revista de Estudos Jurídicos da UNESP**, Franca, v. 18, n. 28, 2015, p. 3.
[323] MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 210.
[324] Ibid., p. 211.

Dentro desse contexto, há nova ordem no sentido de interferências fora do campo tradicionalmente conhecido, de tal sorte que as normas internacionais devem ser analisadas em conjunto com o Estado constitucional, dentro do novo panorama jurídico-social de resolução de conflitos – inclusive no âmbito extrajudicial. Em outras palavras, analisar como eventual unificação pode resultar em um processo célere, que não deixe de observar balizas constitucionais.

A ausência de fronteiras no ambiente digital dificulta a capacidade do Estado de atuar como regulador no mundo físico, em contraste com sua atuação no espaço virtual, o que pode gerar conflitos de jurisdição. Como os impactos reais de uma ferramenta on-line se manifestam em diferentes locais do mundo, as ações de pessoas conectadas à internet podem estar sujeitas a uma jurisdição diferente daquela em que os dados foram utilizados, algo que a maioria dos usuários desses sites desconhece[325].

A questão pode ser abordada pela ótica do Direito Internacional Privado, inclusive. No entanto, a questão é a dificuldade de fazer cumprir decisões judiciais quando se trata de empresas estrangeiras, que frequentemente escolhem estabelecer suas sedes em localidades vantajosas[326].

Acerca do tema:

> Quanto aos princípios positivos que conduzem à competência internacional, o princípio de acesso à Justiça e inafastabilidade do controle jurisdicional surge como argumento relevante, utilizado, por vezes, em decisões judiciais brasileiras que envolvem elementos estrangeiros, como, por exemplo, em ações relativas a empresas com sede no exterior.
> O princípio da *plenitudo jurisdictionis* também é especialmente relevante, pois determina a soberania do Estado para definir a sua própria competência (ou jurisdição) sobre uma lide, fazendo com que os aspectos processuais e procedimentos sejam regidos exclusivamente pela *lex fori*.
> O princípio da autonomia da vontade pode ser aplicado para reconhecer a validade de cláusulas contratuais de eleição de foro, como manifestação da vontade das partes quando da sua celebração, ou então, pode ser afastado, especialmente no caso de demandas que envolvem direito do consumidor, de modo que a abusividade eventual de cláusulas de eleição de foro demanda, necessariamente, a análise de elementos fáticos.
> Isto porque, ainda que conste eleição de foro diverso no contrato celebrado entre as partes, aplicar-se-á o art. 101, inc. I do Código de Defesa do Consumidor, o que permite o ajuizamento da ação no domicílio do autor. Deste modo, se o autor for consumidor domiciliado no Brasil, o Judiciário brasileiro poderá ser reconhecido como competente para solucionar controvérsias decorrentes do contrato, independentemente do foro previsto no instrumento celebrado.
> A proteção assegurada pelo CDC é essencial para garantir o acesso à Justiça dos consumidores que contratam produtos ou serviços pela Internet. Por vezes, enquanto o consumidor é brasileiro e está aqui domiciliado, o site pelo qual é feita a contratação

[325] MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 212.
[326] Ibid., p. 216.

> está registrado em outro país, seus servidores localizados em outro e a sede da empresa ainda em outro.
> Soma-se a isto o fato de que muitas contratações são feitas a partir da assinatura de termos automáticos, termos de aceite ou de uso e condições – os quais raramente são lidos e compreendidos em sua integridade pelo consumidor. Ainda que conste cláusula expressa elegendo foro estrangeiro, não é possível afirmar que se trata de vontade comum das partes ou expressão de sua autonomia, já que o consumidor, parte hipossuficiente, dificilmente estava ciente de tal aspecto quando realizou a contratação.
> Tal princípio esbarra, por vezes, com o princípio da efetividade, disposto entre os princípios negativos de incidência da jurisdição internacional do Estado. Isto porque, mesmo que seja possível o ajuizamento da demanda perante o Judiciário brasileiro, a jurisdição nacional encontra limites quanto à possibilidade de cumprimento de decisões[327].

A título de exemplo, a recente decisão de Alexandre de Moraes pela suspensão imediata da plataforma "X" (antigo Twitter) no Brasil. Nesta, o primeiro ponto a ser observado é a admissão de medidas cautelares não previstas em lei (poder geral de cautela no âmbito do processo penal). Assim, diante do não cumprimento da determinação de remoção do site, houve imposição de multa. A decisão foi tomada porque a referida rede social estaria desrespeitando normas estabelecidas pela Justiça brasileira:

> EMENTA: CONSTITUCIONAL E CIVIL. NOVA REALIDADE NA INSTRUMENTALIZAÇÃO DAS REDES SOCIAIS PELOS POPULISTAS DIGITAIS EXTREMISTAS COM MACIÇA DIVULGAÇÃO DE DISCURSOS DE ÓDIO E MENSAGENS ANTIDEMOCRÁTICAS. UTILIZAÇÃO DE DESINFORMAÇÃO PARA CORROER OS PILARES DA DEMOCRACIA E DO ESTADO DE DIREITO. NECESSIDADE DE ABSOLUTO RESPEITO AOS PRINCÍPIOS E OBJETIVOS DA REPÚBLICA (CF. ARTS. 1º, 2º E 3º) POR TODAS AS EMPRESAS NACIONAIS OU ESTRANGEIRAS. OBRIGATORIEDADE LEGAL DE NOMEAÇÃO DE REPRESENTANTE LEGAL DE EMPRESA QUE ATUE EM TERRITÓRIO NACIONAL. OBRIGATORIEDADE CONSTITUCIONAL DE RESPEITO ÀS DECISÕES DO PODER JUDICIÁRIO. OSTENSIVA REITERAÇÃO DE DESOBEDIENCIA À ORDEM JUDICIAL CARACTERIZADA. DECISÃO REFERENDADA.
> 1. A Constituição da República Federativa do Brasil de 1988 não permite que se confunda liberdade de expressão com liberdade de agressão ou inexistente censura com necessária proibição constitucional ao discurso de ódio e de incitação a atos antidemocráticos.
> 2. Toda e qualquer entidade privada que exerça sua atividade econômica em território nacional deve respeitar o ordenamento jurídico nacional e cumprir, de forma efetiva, comandos diretos emitidos pelo Poder Judiciário brasileiro.
> 3. O Código Civil brasileiro estabelece que a constituição de qualquer sociedade, obrigatoriamente, deve indicar as pessoas naturais incumbidas da administração da sociedade, e seus poderes e atribuições.
> 4. A sociedade estrangeira, para poder atuar legalmente no Brasil, necessita de autorização prévia do governo federal (LINDB, art. 11, § 2º), com expressa indicação de representante no Brasil, com poderes para resolver quaisquer questões e receber citação judicial pela sociedade (CC, art. 1.138) e, uma vez autorizada a funcionar, ficará sujeita às leis e aos tribunais brasileiros, quanto aos atos ou operações praticados no Brasil (CC, art. 1.137).

[327] MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 220-221.

> 5. O Marco Civil da Internet (Lei 12.965/2014) prevê a responsabilização civil do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, caso não sejam realizadas as medidas determinadas por ordem judicial dentro do prazo assinalado e nos limites técnicos do serviço.
> 6. Esgotamento de todos os mecanismos legais para que a empresa X BRASIL cumprisse as ordens judiciais, no intuito de impedir medida mais gravosa.
> 7. Manutenção ostensiva e agressiva do desrespeito às ordens judiciais do Poder Judiciário brasileiro, com o encerramento das atividades da X BRASIL em território nacional, com a não nomeação de representantes legais, não adimplemento das multas aplicadas e, inclusive, por meio de inúmeras postagens ofensivas reiterando o desprezo pelo JUSTIÇA BRASILEIRA.
> 8. Presença dos requisitos legais necessários, fumus boni iuris consistente nos reiterados, conscientes e voluntários descumprimentos das ordens judiciais e inadimplemento das multas diárias aplicadas, além da tentativa de não se submeter ao ordenamento jurídico e Poder Judiciário brasileiros, para instituir um ambiente de total impunidade e terra sem lei nas redes sociais brasileiras, inclusive durante as eleições municipais de 2024 , bem como o periculum in mora consistente na manutenção e ampliação da instrumentalização da X BRASIL, por meio da atuação de grupos extremistas e milícias digitais nas redes sociais, com massiva divulgação de discursos nazistas, racistas, fascistas, de ódio, antidemocráticos, inclusive no período que antecede as eleições municipais de 2024.

Posteriormente, foi autorizado o retorno do "X", diante do cumprimento das condições estipuladas, com determinação para que a Anatel adotasse providências para sua retomada[328].

Fato é que no âmbito das relações digitais, todas as características tradicionalmente estabelecidas à jurisdição devem ser analisadas sob um novo viés.

Nesse sentido, Amanda Martins destaca:

> Com o Regulamento Geral de Proteção de Dados, a jurisdição internacionalmente competente em demandas que envolvem o meio digital ficou mais clara. Especialmente relevantes tais disposições, já que a localização geográfica dos dados armazenados, por exemplo, em nuvem (*cloud*), poderá determinar o cumprimento de regulação específica de um país ou grupo de países. Existe, portanto, certa flexibilidade na definição da jurisdição competente.
> Em casos que envolvem responsabilidade de autoridades de um Estado-Membro no exercício dos seus poderes públicos, ou seja, envolvendo uma agência de controle governamental, a ação deverá necessariamente ser ajuizada perante os tribunais daquele Estado-Membro, nos termos do art. 78. Já os casos que visam reparação por violações ao Regulamento, cuja responsabilidade é de empresas privadas, devem observar o art. 79.
> Em tais hipóteses, há a possibilidade de diversos tribunais serem efetivamente competentes, o que poderá suscitar questões de litispendência (abordadas, por sua vez, no art. 81). Conforme mencionado, o art. 79 dispõe sobre a jurisdição ou a competência internacional, determinando que será competente, em princípio, o Tribunal do local onde o responsável pelo tratamento, ou subcontratante, tenha estabelecimento.
> Abre-se a possibilidade de ajuizamento, portanto, em qualquer Estado-Membro no qual a empresa esteja estabelecida, não havendo distinção, segundo o Regulamento, entre estabelecimento e estabelecimento principal. Há, ainda, o reconhecimento da

[328] STF NOTÍCIAS. STF autoriza retorno imediato do X e determina que Anatel adote providências para retomada do serviço. **STF Notícias,** 8 out. 2024. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-autoriza-o-retorno-imediato-do-x-e-determina-que-anatel-adote-providencias-para-a-retomada-do-servico/. Acesso em: 11 out. 2024.

> competência do Tribunal do local de residência habitual do demandante, inclusive na hipótese de a empresa não possui estabelecimento em território na União Europeia.
> As possibilidades de foros competentes para ajuizar demandas do gênero no âmbito do RGPD são, portanto, múltiplas. Verificada a ocorrência de litispendência, a ação poderá ser suspensa ou extinta, mas em ambos os casos visa evitar que sejam prolatadas decisões conflitantes ou inconciliáveis (art. 81).
> Para além do âmbito da responsabilidade civil, o RGPD é aplicável ao tratamento de titulares de dados que se encontrem no território da União, mesmo se o responsável pelo tratamento dos dados ou subcontratante não estiver estabelecido na U.E., nas hipóteses referidas no art. 3º do Regulamento[329].

No Brasil, o artigo 26 do Código de Processo Civil trata da cooperação jurídica internacional, regida por tratado de que o Brasil faça parte, observando: (i) "o respeito às garantias do devido processo legal no Estado requerente"; (ii) "a igualdade de tratamento entre nacionais e estrangeiros, residentes ou não no Brasil, em relação ao acesso à justiça e à tramitação dos processos, assegurando-se assistência judiciária aos necessitados"; (iii) "a publicidade processual, exceto nas hipóteses de sigilo previstas na legislação brasileira ou na do Estado requerente"; (iv) "a existência de autoridade central para recepção e transmissão dos pedidos de cooperação"; e (v) "a espontaneidade na transmissão de informações a autoridades estrangeiras".

Ainda, na ausência de tratado, a cooperação jurídica internacional será realizada com base em reciprocidade, manifestada por via diplomática (art. 26, § 1º).

A noção clássica de soberania, assim como a de privacidade, tem passado por mudanças significativas, o que gera dificuldades para definir como a jurisdição estadual se aplica em um espaço geográfico específico. Assim, ao navegarem na internet, as pessoas frequentemente não percebem que estão realizando atividades sob as normas de uma jurisdição que não é a mesma do local onde estão conectados. Nesse contexto, existem critérios específicos que definem a jurisdição em situações que envolvem a internet. A principal característica desses critérios de conexão é que eles evidenciam uma ligação objetiva ou territorial da questão a um determinado Estado, considerando aspectos como o local onde uma obrigação foi cumprida, o local de formalização de um contrato, a nacionalidade ou domicílio das partes, e o local onde o dano ocorreu, entre outros fatores. O segundo ponto diz respeito ao caráter rígido e neutro dos critérios tradicionais do Direito Internacional Privado, que se baseiam em conceitos jurídicos claramente definidos. Embora essa neutralidade possa ser benéfica na resolução de conflitos em situações concretas, a inflexibilidade desses critérios, quando comparada à natureza

[329] MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 225-226.

dinâmica das questões que surgem na internet, pode, em várias ocasiões, dificultar uma solução eficaz[330].

A definição dos critérios de conexão relevantes e a subsequente determinação da legislação aplicável constituem um desafio significativo. As normas de conflitos, ao se fundamentarem em regras clássicas ou atuais de conexão que possuem um caráter essencialmente localizado (em contraste com a deslocalização proporcionada pela internet), podem, em algumas situações, revelar-se inadequadas. No entanto, isso não implica que essas normas sejam inelegíveis para resolver disputas no ambiente digital. Embora as fronteiras geográficas convencionais não se ajustem à realidade da internet, os fundamentos clássicos do Direito Internacional Privado têm ligação com ações que possuem uma presença física, em vez de serem meramente virtuais. O desafio apresentado atualmente traz novos obstáculos, exigindo, em algumas ocasiões, a busca por respostas que sejam igualmente criativas. Ademais, é viável empregar critérios de conexão e princípios que são comumente aplicados no Direito Internacional Privado, bem como conceitos e princípios que já estão firmemente estabelecidos no Direito Civil[331].

No campo penal/processual penal, a Polícia Federal conta com Coordenação-Federal de Cooperação Internacional, vinculada à Diretoria Executiva, com combate aos crimes informáticos. Nesse sentido:

> Polícia Federal se utiliza da cooperação internacional como instrumento para combater de maneira eficaz a criminalidade organizada transnacional e para preservar a segurança interna. Para tanto, formaliza parcerias com instituições estrangeiras, fomentando a cooperação e assistência mútuas.
> A polícia de cooperação da Polícia Federal baseia-se na reciprocidade e nos interesses mútuos e tem por objetivo a transferência de conhecimentos e informações, realização de ações conjuntas e capacitação de policiais [...][332].

Vale destacar que existem diversos acordos multilaterais e bilaterais do Brasil em matéria penal, que podem ser encontrados no sítio do Ministério da Justiça[333].

---

330 MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022, p. 232-233.
331 Ibid., p. 233-234.
332 POLÍCIA FEDERAL. Acordo de Cooperação Internacional. **Ministério da Justiça e Segurança Pública.** Disponível em https://www.gov.br/pf/pt-br/assuntos/acordos-de-cooperacao#:~:text=Pol%C3%ADcia%20Federal%20se%20utiliza%20da,a%20coopera%C3%A7%C3%A3o%20e%20assist%C3%AAncia%20m%C3%BAtuas. Acesso em: 11 out. 2024.
333 BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. **Manual de Cooperação Jurídica Internacional: Matéria Penal e Recuperação de Ativos**. 4. ed., 2019. Disponível em https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagem-de-dinheiro/drci/publicacoes/manuais/cooperacao-juridica-internacional-em-materia-penal/manual-penal-online-final-2.pdf. Acesso em: 11 jul. 2024.

Segundo o STJ, a cooperação jurídica internacional é um compromisso assumido pelo Estado brasileiro:

> Com base na legislação vigente, qualquer país pode solicitar às autoridades brasileiras a execução de medidas administrativas, investigativas ou judiciais necessárias num caso concreto em andamento.
> Esse mecanismo, amparado em normas e tratados além-mar, visa assegurar a eficácia das leis nacionais e internacionais, sempre que necessária a realização de atos em território estrangeiro.
> No Brasil, o Ministério da Justiça e Segurança Pública exerce a função de autoridade central do sistema de cooperação jurídica internacional, sendo o destinatário de demandas que costumam ser intermediadas por vias diplomáticas. Cabe a ele classificar as solicitações recebidas, de acordo com a natureza do pleito, e dar o devido encaminhamento.
> Se o pedido envolver a prática de um ato judicial, o caso poderá ser remetido ao STJ em forma de carta rogatória (para determinar a adoção de diligências processuais) ou de ação de homologação de decisão estrangeira (para fazer cumprir no Brasil a sentença proferida pela Justiça de outro país).
> Nas cartas rogatórias, o STJ só procede à concessão do *exequatur* (autorização para cumprimento da medida solicitada) após examinar a compreensibilidade do caso e a possibilidade de ofensa à soberania nacional, à ordem pública ou à dignidade da pessoa humana.
> Nas situações em que o cumprimento de medidas de cooperação jurídica no exterior é requerido pelas autoridades brasileiras – sejam elas investigativas, administrativas ou judiciais –, o procedimento não passa pelo STJ. Nesses casos, o encaminhamento do pedido pelo magistrado é feito diretamente através do Ministério da Justiça e Segurança Pública, que também exerce a função de autoridade central para pedidos de cooperação ativos[334].

Em relação aos crimes cibernéticos e a competência, Erika Pigatin destaca:

> Conhecer o lugar do crime é essencial para a aplicação ou não da lei brasileira e também para a fixação da comarca ou subseção competente. Apesar de a territorialidade ser regra, o ordenamento penal brasileiro também utiliza a teoria da ubiquidade ou mista, agasalhada pelo artigo 6º em que "considera-se praticado o crime no lugar em que ocorrer a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado". Sendo assim, podemos considerar que o delito foi realizado no lugar onde foi produzida a conduta criminal (no nosso país, por exemplo), também no lugar onde foi produzido ou deveria ser produzido o resultado (nesse caso, fora do território brasileiro, por exemplo).
> No caso de crimes em que a ação e também a consumação ocorra em lugares diferentes, porém ambos praticados em território nacional podemos nos valer da regra do artigo 10, caput, do Código de Processo Penal, que diz que "a competência será, de regra, determinada pelo lugar em que se consumar e infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução" fazendo com que a competência, neste caso seja fixada, pelo lugar da consumação do delito de acordo com a teoria do resultado.
> Devemos levar em consideração que em determinados delitos perpetrados com o uso da internet são consumados em todos os lugares onde exista a rede disponível. Um crime praticado contra a honra, a injúria, por exemplo, onde o agente denigre a dignidade ou decoro de uma pessoa através de declarações insultuosas na rede, esse crime pode ser conhecido por qualquer pessoa do mundo, bastando que ela acesse a

[334] STJ. **Cooperação Jurídica Internacional.** Disponível em https://international.stj.jus.br/pt/Cooperacao-Internacional/Cooperacao-Juridica-Internacional. Acesso em: 10 out. 2024.

> página na internet. Nesse caso a determinação do foro da culpa é quase que impossível[335].

A empresa transnacional surge dentro do sistema capitalista, com operações de modo globalizado, com atuação que implica acordos entre diversos Estados. A atividade, portanto, não pode ser realizada à margem dos próprios direitos humanos no espaço internacional.

Existe, portanto, uma confluência de valores e metas a serem atingidas, da mesma forma que é necessária a regulamentação própria para que não permaneçam lacunas que acabem ensejando retrocesso.

A evolução empresarial deve caminhar junto com a humanidade. Os movimentos avistados que culminaram em garantias constitucionais que existem hoje não podem ser deixados de lado em prol do crescimento do capital. Da mesma forma, esse crescimento não pode ser ignorado.

São diversas facetas e diversas problemáticas que se evidenciam à medida em que o tema é estudado.

O tratamento de dados, mais especificamente, seu armazenamento, como é possível ser feita sua consulta e sua disposição? Quais os cuidados que devem ser tomados? São apenas alguns dos questionamentos que devem ser levados em conta sobretudo na estrutura e sistematização das empresas. E, como consequência, tais pontos serão levados também em consideração na própria incidência do Direito Penal.

5.2 CONVENÇÃO DE BUDAPESTE (CONVENÇÃO SOBRE O CIBERCRIME) E SUA RECENTE PROMULGAÇÃO NO BRASIL

A Convenção sobre o Cibercrime (firmada em Budapeste, em 23 de novembro de 2001), foi promulgada no Brasil, com o Decreto nº 11.491, publicado no Diário Oficial da União (DOU), no dia 12 de abril de 2023, de tal sorte que as autoridades brasileiras podem, portanto, contar com mais um recurso nas investigações de crimes cibernéticos ou outras infrações penais que demandam a obtenção de provas digitais armazenadas em outros países.

Foi estabelecido um tratado internacional de direito penal e de processo penal no contexto do Conselho da Europa em 2001, com a finalidade de harmonizar a definição de crimes

---

[335] PIGATIN, Erika. Crimes Cibernéticos. **JusBrasil,** 2019. Disponível em https://www.jusbrasil.com.br/artigos/crimes-ciberneticos/747423400?_gl=1*iiruz6*_gcl_aw*R0NMLjE3MjU5MDE0NTUuQ2p3S0NBand1ZnEyQmhBbUVpd0FuWnF3OHZwRE1ZbTlkc1p1aDQ3OXItRmdJNXJhUVdSdUxnVXItS0UyU0lmZUlHelNXLTJaeEpsMnRSb0NwMXNRQXZEX0J3RQ..*_gcl_au*MjgzMTc2MzM3LjE3MjIyNjU2MjM.*_ga*MTM3ODY2ODEzLjE2NjU3NDA3MzE.*_ga_QCSXBQ8XPZ*MTcyODQwMzM5MC4xODcuMC4xNzI4NDAzMzkwLjYwLjAuMA. Acesso em: 09 out. 2024.

cometidos pela internet e as metodologias de investigação, buscando assim uma abordagem coesa no enfrentamento dessa modalidade de criminalidade. Devido à natureza transnacional desse tipo de crime, é fundamental que diferentes Estados colaborem para prevenir e combater essas infrações[336].

Nesse sentido, consta de seu preâmbulo que:

> [...] é necessária para impedir ações conduzidas contra a confidencialidade, a integridade e a disponibilidade de sistemas informáticos, redes e dados de computador, bem como para impedir o abuso de tais sistemas, redes e dados, ao prever a criminalização de tais condutas, tal como se encontram descritas nesta Convenção, e ao prever a criação de competências suficientes para combater efetivamente tais crimes, facilitando a descoberta, a investigação e o julgamento dessas infrações penais em instâncias domésticas e internacionais, e ao estabelecer mecanismos para uma cooperação internacional rápida e confiável.

Um dos pontos importantes é a questão da responsabilidade da pessoa jurídica por crimes cibernéticos, sendo possível a responsabilidade, com base: "a. no poder de representação da pessoa jurídica; b. na autoridade de tomar decisões em nome da pessoa jurídica; c. na autoridade de exercer controle interno na pessoa jurídica" (art. 12).

Como se vê, o modelo proposto é atrelado ao crime praticado pela pessoa física. De todo modo, é certo que existe previsão constitucional acerca da responsabilidade penal da pessoa jurídica. Nesse sentido, o art. 173, § 5º da CF/88 prevê a responsabilidade "sujeitando-a às punições compatíveis com sua natureza, nos atos praticados contra a ordem econômica e financeira e contra a economia popular" e, no art. 225, § 3º, que "as condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados".

Não se olvida da discussão acerca de tal possibilidade, notadamente pela historicidade que remonta ao *societas delinquere non potest*, mas o desenvolvimento teórico da responsabilidade penal das pessoas jurídicas desagua na sua viabilidade. No mais, é ponto que (certamente) engendrará discussões atreladas à própria sanção e rito.

Outro tópico importante é a questão da preservação expedida de dados armazenados em computador sendo que cada parte deverá adotar medidas necessárias para tanto, incluindo dados de tráfego que tenham sido armazenados por meio de sistema de computador, "especialmente

---

[336] MOURA, Grégore Moreira de. **Curso de Direito Penal Informático**. Belo Horizonte, São Paulo: D'Plácido, 2021, p. 37.

quando haja razões para admitir que os dados de computador estão particularmente sujeitos à perda ou modificação" (art. 16).

A documentação de conservação de informações é recurso que visa obtenção de provas para posterior utilização, pensando em futura prova dentro de um processo penal. A importância ocorre porque uma das características da evidência digital é justamente sua volatilidade, por isso o armazenamento, com o fim de preservar eventuais mudanças.

Além disso, há a autorização aos Estados signatários de adotarem medidas legislativas para permitir o acesso (art. 18[337]). A importância desse procedimento reside no fato de que as autoridades conseguem obter informações essenciais para a investigação de crimes com a colaboração do responsável pela posse desses dados. Dessa forma, mesmo existindo outras maneiras de acessar essas informações, como a busca e apreensão, as diversas formas de esconder os dados e impedir o acesso a eles podem resultar na falta de sucesso das investigações.

Nesse meio de obtenção de prova, o Estado terá diversas prerrogativas, como apreender ou obter o sistema informático, efetuar e conservar cópia de tais dados, além de preservar sua integridade (art. 19[338]).

---

[337] Artigo 18 - Ordem de exibição. 1. Cada Parte adotará as medidas legislativas e outras providências necessárias para dar poderes a autoridades competentes para ordenar: a. a qualquer pessoa residente em seu território a entregar dados de computador especificados, por ela controlados ou detidos, que estejam armazenados num sistema de computador ou em qualquer meio de armazenamento de dados de computador; b. a qualquer provedor de serviço que atue no território da Parte a entregar informações cadastrais de assinantes de tais serviços, que estejam sob a detenção ou controle do provedor. 2. Os poderes e procedimentos referidos neste artigo estão sujeitos aos Artigos 14 e 15. 3. Paras os fins deste Artigo, o termo "informações cadastrais do assinante" indica qualquer informação mantida em forma eletrônica ou em qualquer outra, que esteja em poder do provedor de serviço e que seja relativa a assinantes de seus serviços, com exceção dos dados de tráfego e do conteúdo da comunicação, e por meio da qual se possa determinar: a. o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas para esse fim e a época do serviço; b. a identidade do assinante, o domicílio ou o endereço postal, o telefone e outros números de contato e informações sobre pagamento e cobrança, que estejam disponíveis de acordo com o contrato de prestação de serviço. c. quaisquer outras informações sobre o local da instalação do equipamento de comunicação disponível com base no contrato de prestação de serviço.

[338] Artigo 19 - Busca e apreensão de dados de computador - 1. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes para busca ou investigação, em seu território: a. de qualquer sistema de computador ou de parte dele e dos dados nele armazenados; e b. de qualquer meio de armazenamento de dados de computador no qual possam estar armazenados os dados procurados em seu território. 2. Cada Parte adotará medidas legislativas e outras providências necessárias para assegurar que, quando a autoridade competente proceder a busca em um determinado sistema de computador ou em parte dele, de acordo com o parágrafo 1.a, e tiver fundadas razões para supor que os dados procurados estão armazenados em outro sistema de computador ou em parte dele, situado em seu território, e que tais dados são legalmente acessíveis a partir do sistema inicial, ou disponíveis a esse sistema, tal autoridade poderá estender prontamente a busca ou o acesso ao outro sistema. 3. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes para apreender ou proteger dados de computador acessados de acordo com os parágrafos 1 ou 2. Estas medidas incluirão o poder de: a. apreender ou proteger um sistema de computador ou parte dele ou um meio de armazenamento de dados; b. fazer e guardar uma cópia desses dados de computador;
c. manter a integridade dos dados de computador relevantes; d. tornar inacessíveis esses dados no sistema de computador acessado ou dele removê-los. 4. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a sua autoridade competente para determinar que qualquer pessoa que conheça o

O título 5 da Convenção trata da obtenção de dados de computador em *tempo real* (artigos 20 e 21[339]). É válido ressaltar a necessidade de haver métodos específicos para coletar provas digitais devido ao uso crescente de sistemas computacionais na prática de diversos crimes. Isso se deve ao fato de que tais sistemas facilitam a transmissão de dados de diferentes formas (por exemplo, texto, imagem, som, etc.) e também possibilitam a eliminação de provas digitais, que são voláteis por natureza. Geralmente, apenas especialistas em Ciência Forense Digital têm a capacidade de entender as particularidades das provas digitais[340].

Um aspecto significativo abordado na Convenção é a definição da autoridade responsável pela penalização desses delitos. Os crimes cibernéticos não estão restritos a uma única localização geográfica, o que pode gerar grandes desafios na investigação e na determinação da jurisdição apropriada para o seu julgamento, como já dito. Por essa razão, a Convenção estabelece as normas de jurisdição, assegurando, tal como faz o Código Penal brasileiro, a aplicação da regra geral do princípio da territorialidade moderada. Aqui, a

---

funcionamento do sistema de computador ou as medidas empregadas para proteger os dados nele armazenados que forneça, tanto quanto seja razoável, as informações necessárias para permitir as providências referidas nos parágrafos 1 e 2. 5. Os poderes e procedimentos referidos neste artigo estarão sujeitos aos dispositivos dos Artigos 14 e 15.

[339] Artigo 20 - Obtenção de dados de tráfego em tempo real - 1. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes, no que seja pertinente a dados de tráfego, em tempo real, vinculados a comunicações específicas, ocorridas em seu território, por meio de um sistema de computador, para: a. coletar tais dados ou gravá-los por meios técnicos, no território da Parte, e b. obrigar um provedor de serviço, nos limites de sua capacidade técnica: i. a reunir tais dados ou gravá-los por meios técnicos, no território da Parte; ou ii. a cooperar com as autoridades competentes ou auxiliá-las na obtenção ou gravação de tais dados. 2. Quando uma Parte, em razão dos princípios legais de seu sistema jurídico, não puder adotar as medidas referidas no parágrafo 1.a., a Parte poderá substituí-las por medidas legislativas e outras providências necessárias para assegurar a obtenção ou a gravação em tempo real, por meios técnicos aplicados em seu próprio território, dos dados de tráfego vinculados a uma comunicação específica, transmitida nesse território. 3. Cada Parte adotará medidas legislativas e outras providências necessárias para obrigar um provedor de serviço a manter em sigilo a execução de qualquer das atribuições investigativas estabelecidas neste Artigo e quaisquer informações relativas a elas. 4. Os poderes e procedimentos referidos neste Artigo obedecerão aos Artigos 14 e 15.
Artigo 21 - Interceptação de dados de conteúdo - 1. Cada Parte adotará medidas legislativas e outras providências necessárias, em relação a um conjunto de crimes graves a serem especificados pela legislação doméstica, e no que seja pertinente ao conteúdo de comunicações específicas, ocorridas em seu território, por meio de um sistema de computador, para dar poderes a suas autoridades competentes, a fim de que possam, em tempo real: a. coletar ou gravar tais comunicações, por meios técnicos, no território dessa Parte, e b. compelir um provedor de serviço, nos limites de sua capacidade técnica: i. a coletar ou gravar tais comunicações, por meios técnicos, no território dessa Parte; ou ii. a cooperar com as autoridades competentes, ou ajudá-las, na obtenção ou gravação do conteúdo dessas comunicações. 2. Quando uma Parte, em razão dos princípios legais de seu sistema jurídico, não puder adotar as medidas referidas no parágrafo 1.a., a Parte poderá substituí-las por medidas legislativas e outras providências necessárias para assegurar a obtenção ou a gravação em tempo real, por meios técnicos aplicados em seu próprio território, do conteúdo de comunicações específicas transmitidas nesse território. 3. Cada Parte adotará medidas legislativas e outras providências necessárias para obrigar um provedor de serviço a manter em sigilo a execução de qualquer das atribuições investigativas estabelecidas neste Artigo e quaisquer informações relativas a elas.
4. Os poderes e procedimentos referidos neste Artigo obedecerão aos Artigos 14 e 15.

[340] KIST, Dario José. **Prova Digital no Processo penal**. Leme, SP: JH Mizuno, 2019, p. 183.

jurisdição possui um componente espacial ou territorial, mas é ajustada por aspectos como a nacionalidade, a bandeira ou outros fatores[341]. Assim estabelece o artigo 22:

> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para estabelecer jurisdição sobre qualquer dos crimes tipificados de acordo com os Artigos de 2 a 11 desta Convenção, quando a infração for cometida:
> a. no seu território; ou
> b. a bordo de uma embarcação de bandeira dessa Parte; ou
> c. a bordo de uma aeronave registrada conforme as leis dessa Parte; ou
> d. por um seu nacional, se o crime for punível segundo as leis penais do local do fato ou se o crime for cometido fora da jurisdição de qualquer Parte.
> 2. Qualquer Parte pode reservar-se o direito de não aplicar ou aplicar somente em casos específicos ou em condições especiais as regras de jurisdição assentadas nos parágrafos 1.b a 1.d deste Artigo ou qualquer parte delas.
> 3. Cada Estado adotará medidas necessárias para estabelecer jurisdição sobre os crimes referidos no Artigo 24, parágrafo 1, desta Convenção, quando um suspeito da prática de tais crimes estiver em seu território e esta Parte não o extradite para outra Parte, somente em razão de sua nacionalidade, depois de um pedido de extradição.
> 4. Esta Convenção não exclui nenhuma espécie de jurisdição criminal exercida pela Parte de acordo com a sua legislação doméstica.
> 5. Se mais de uma Parte reivindicar jurisdição sobre suposto crime previsto nesta Convenção, as Partes envolvidas, quando conveniente, deverão promover consultas para determinar a jurisdição mais adequada para o processo.

A tecnologia normativa busca prevenir a impunidade e favorecer a cooperação entre as partes, observando as diretrizes de jurisdição e competência, e, sobretudo, as disposições constitucionais de cada país, pois estas geralmente estabelecem as regras relacionadas à extradição e nacionalidade de forma ampliada. A complexidade das evidências em crimes cibernéticos e sua extensão por diversos países requer uma ação rápida e decisiva na coleta e no armazenamento das provas. Da mesma forma que em delitos tradicionais, é crucial manter a integridade da cena do crime para garantir a eficácia da investigação e o êxito do processo, o que se aplica igualmente aos crimes informáticos[342].

Dos artigos 23 ao 35 da Convenção de Budapeste extraem-se relevantes novidades acerca da cooperação jurídica internacional para obtenção de provas digitais, com o objetivo de maior eficiência.

Nesse sentido, o artigo 25.3, ao tratar da assistência mútua, estabelece:

> Cada Parte pode, em casos urgentes, solicitar assistência mútua ou fazer comunicados relativos a ela por meios de comunicação rápida, inclusive por fax ou email, desde que tais meios proporcionem níveis adequados de segurança e autenticidade (incluindo o uso de criptografia, se necessário), com posterior confirmação formal, se

[341] MOURA, Grégore Moreira de. **Curso de Direito Penal Informático**. Belo Horizonte, São Paulo: D'Plácido, 2021, p. 4-49.
[342] Ibid., p. 49-50.

> exigida pela Parte requerida. A Parte requerida aceitará e atenderá ao pedido por qualquer meio de comunicação expedito.

Para fortalecer as relações com outros Estados, a aprovação de um acordo que regula a colaboração em relação às provas digitais era algo necessário há muito tempo. Isso porque as provas digitais possuem peculiaridades (como volatilidade e dispersão) que as diferenciam das provas físicas, exigindo procedimentos de cooperação específicos para sua obtenção.

Ora, atualmente, as informações on-line podem ser acessadas remotamente de qualquer lugar (nuvem), mas que muitas vezes estão fisicamente armazenadas em país diferente daquele em que o usuário se encontra. Além disso, as informações em si são transfronteiriças ou não territoriais, pois são facilmente transferidas entre países, divididas e replicadas em locais distintos e por vezes não se sabe ao certo onde estão localizadas.

Assim, com o fim de conferir maior celeridade, a Convenção prevê instrumentos cautelares: conservação de dados armazenados quando há risco de perda ou modificação (art. 29) e revelação de dados específicos para identificação do provedor (art. 30).

Além disso, elenca instrumentos para obtenção de prova digital: busca, acesso, apreensão, guarda ou revelação de dados (art. 31), pedido de intercepção de dados em tempo real (art. 33) e interceptação ou gravação em tempo do conteúdo de comunicações (art. 34).

E, não menos importante, o art. 32 estabelece as hipóteses para acesso transfronteiriço, nos seguintes termos:

> Uma Parte poderá, sem a autorização de outra Parte:
> a. **acessar dados de computador disponíveis ao público** (fonte aberta), **independentemente de onde os dados estejam geograficamente localizados**; ou
> b**. acessar ou receber, por meio de um sistema de computador em seu território, dados de computador armazenados no território de outra Parte**, **se a Parte obtiver o legítimo e voluntário consentimento de uma pessoa que tenha autoridade legal para revelar os dados à Parte interessada**, por meio de um sistema de computador (grifos nossos).

Aqui, certa atenção deve ser despendida, para que não haja excesso na utilização de referido dispositivo, dada a natureza unilateral, o que deverá, contudo, ser objeto de análise no caso concreto.

Dessa forma, o Brasil, ao aceitar o convite do Conselho da Europa, passa a ser um dos países que aderiram ao referido instrumento, com a cooperação no enfrentamento aos crimes cibernéticos[343]. Afinal, haverá melhora no arcabouço legal para obtenção de provas digitais,

[343] Pois a Convenção abarca mais de 60 países.

notadamente diante da possibilidade do acesso transfronteiriço a provas, mas com preservação da soberania nacional.

No entanto, como se viu, mesmo com a Convenção tendo status de lei federal e o legislativo brasileiro reconhecendo a gravidade desses atos, a investigação criminal encontra alguns óbices devido à proteção do princípio da legalidade, que exige regulamentação legal para que as ações propostas sejam efetivamente aplicadas, seja pela definição precisa dos crimes a serem punidos, seja pela estipulação das penas possíveis a serem impostas.

É crucial ter cautela ao definir novos comportamentos introduzidos pela Convenção, a fim de evitar a sobreposição com os crimes já estabelecidos na lei brasileira ou um excesso de punição. A avaliação do interesse jurídico, a definição clara do crime e a imposição de penas adequadas são passos essenciais que requerem um debate com um certo nível de maturidade, para que não se torne ineficaz, gerando incerteza jurídica e abrindo espaço para abusos no exercício do poder do Estado.

Com as premissas destacadas, em consonância com a crescente aderência tecnológica, é certo que serão enfrentadas as novas demandas sociais e os instrumentos jurídicos à justiça criminal, com verdadeiras mudanças estruturais. Todas essas questões são analisadas com o fim de viabilizar uma melhor sistematização do tema, esmiuçando o conceito da aderência tecnológica à justiça criminal.

5.3 ACORDO DE ASSISTÊNCIA JUDICIÁRIA EM MATÉRIA PENAL (MLAT)

Considerando que existem empresas que oferecem serviços no Brasil, mas que estão sediadas no exterior, é necessário que a polícia requeira auxílio diplomático (*Mutual Legal Assistance Treaties* – MLAT, ou seja, Transferência Internacional de dados e acordos de assistência mútua), com apoio internacional.

Sua utilização visa, em suma, acesso a dados armazenados em provedores situados no exterior ou seu compartilhamento para outras finalidades, como a persecução penal.

No entanto, é um mecanismo que pode não funcionar no momento de obtenção de dados. Dados de 2018 revelam que de 120 pedidos elaborados, entre os anos de 2014 e 2017, sequer saíram do Brasil, outros considerados sem sucesso e outros ainda em andamento[344]. Isto é, a

[344] CANÁRIO, Pedro. Cooperação jurídica com EUA para quebra de sigilo telemático fracassa 77% das vezes. **ConJur,** 8 mar. 2018. Disponível em: https://www.conjur.com.br/2018-mar-08/cooperacao-eua-quebra-sigilo-fracassa-77-vezes/#:~:text=O%20Mlat%20(Acordo%20de%20Assist%C3%AAncia,ao%20governo%20dos%20Estados%20Unidos. Acesso em: 03 maio 2024.

prestação de informações muitas vezes é dificultada por empresas que alegam que esses dados devem ser sempre requeridos por meio de mecanismos de cooperação, como o MLAT, e não de forma direta.

Com efeito, os acordos de assistência mútua revelam-se muito importantes para a transferência internacional de dados – para diversas finalidades, não apenas quanto à persecução penal. Mas, quando se está diante de investigação penal, a celeridade é sempre crucial.

O C. STJ há muito já se inclinava sobre a possibilidade. Nesse sentido, o julgamento do RMS 55.109, em 11/77/2017:

> A mera alegação de que o braço da empresa situado no Brasil se dedica apenas à prestação de serviços relacionados à locação de espaços publicitários, veiculação de publicidade e suporte de vendas não exime a organização de prestar as informações solicitadas, tanto mais quando se sabe que não raras vezes multinacionais dedicadas à exploração de serviços prestados via internet se valem da escolha do local de sua sede e/ou da central de suas operações com o objetivo específico de burlar carga tributária e ordens judiciais tendentes a regular o conteúdo das matérias por elas veiculadas ou o sigilo de informações de seus usuários. 4. Por estar instituída e em atuação no País, a pessoa jurídica multinacional submete-se, necessariamente, às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados requisitados pelo juízo[345].

Posteriormente, a Ação Declaratória de Constitucionalidade n. 51, ajuizada pela Federação das Associações das Empresas de Tecnologia da Informação, requerendo a confirmação da constitucionalidade do Decreto Federal 3.810/2001, que promulgou o Acordo de Assistência Judiciário-Penal entre o Brasil e os Estados Unidos (MLAT) para que seja o caminho a percorrer para informações privadas de usuários. Nesta, o Min. Relator Gilmar Mendes entendeu pela possibilidade de solicitação de dados diretamente a provedores no exterior. Assim relatou:

> [...] o único instrumento cabível para a solicitação de dados eletrônicos é o da cooperação prevista pelo tratado bilateral e as cartas rogatórias. Porém, também considerou possível que as autoridades brasileiras solicitem essas informações diretamente às empresas localizadas no exterior para as atividades de coleta e tratamento de dados que estejam sob a posse ou o controle de empresa com representação no Brasil e para os crimes cometidos por pessoas localizadas em território nacional. Segundo o relator, essas hipóteses estão contidas no artigo 11 do Marco Civil da Internet, que encontra respaldo no artigo 18 da Convenção de Budapeste [...]

---

[345] BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso em Mandado de Segurança Nº55.019-DF. 2017.** Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1667238&num_registro=201702013432&data=20180201&formato=PDF. Acesso em: 10 ago. 2024.

> O ministro observou que, ainda que o STF conclua pela constitucionalidade do modelo do MLAT em complementação às hipóteses de requisição direta de dados eletrônicos transnacionais, o procedimento de requisição e obtenção de dados deve ser aperfeiçoado mediante a celebração de outros tratados e acordos que possibilitem a obtenção dessas informações com maior agilidade e segurança. Diante disso, o relator entendeu que o Supremo deve comunicar essa decisão aos Poderes Legislativo e Executivo para que adotem providências necessárias, como a aprovação do projeto de uma lei geral de proteção de dados para fins penais (LGPD Penal) e a adesão a outros tratados e acordos internacionais bilaterais sobre o tema[346].

É decisão acertada. Afinal, não se está trabalhando com provas ordinárias. Daí porque, o processo penal do modo como se conhece muitas vezes não deverá ser aplicado sem antes uma nova roupagem.

É certo que o tema sobre empresa ou conglomerado transnacional e sua sujeição à soberania brasileira gera constante discussão acerca da viabilidade dos acordos MLAT.

Tudo isso revela, ainda, a necessidade de solução de problemas quanto à jurisdição – afinal, é preciso aferir o local de onde se originou a conexão à internet e diante de um novo contexto acerca da territorialidade.

Como ensina Renato Brasileiro:

> Em matéria penal, deve-se adotar, em regra, o princípio da territorialidade, desenvolvendo-se na justiça pátria o processo e os respectivos incidentes, não se podendo olvidar, outrossim, de eventuais tratados ou outras normas internacionais a que o país tenha aderido, nos termos dos arts. 1º do CPP e 5º, *caput*, do CP. Tem-se, assim, que a competência internacional é regulada ou pelo direito internacional ou pelas regras internas de determinado país, tendo por fontes os costumes, os tratados normativos e outras regras de direito internacional.
> Portanto, não há ilegalidade na utilização, em processo penal em curso no brasil, de informações compartilhadas por força de acordo internacional de cooperação em matéria penal e oriundas de quebra de sigilo bancário determinada por autoridade estrangeira, com respaldo no ordenamento jurídico de seu país, para a apuração de outros fatos criminosos lá ocorridos, ainda que não haja prévia decisão da justiça brasileira autorizando a quebra do sigilo. Portanto, não há ilegalidade na utilização, em processo penal em curso no brasil, de informações compartilhadas por força de acordo internacional de cooperação em matéria penal e oriundas de quebra de sigilo bancário determinada por autoridade estrangeira, com respaldo no ordenamento jurídico de seu país, para a apuração de outros fatos criminosos lá ocorridos, ainda que não haja prévia decisão da justiça brasileira autorizando a quebra do sigilo.
> Aliás, considerando-se que cada país tem a independência para estabelecer quais medidas investigativas se submetem à reserva de jurisdição, como modo de instituir uma cautela adicional à tutela da intimidade de seus cidadãos, revela-se inviável exigir-se uniformidade sobre o tema no regramento dos diversos Estados soberanos, sob pena de se inviabilizar a própria cooperação jurídica internacional. Destarte, não viola a ordem pública brasileira o compartilhamento direto de dados bancários pelos órgãos investigativos mesmo que, no Estado de origem, sejam obtidos sem prévia autorização judicial, *se a reserva de jurisdição não é exigida pela legislação local*.
> A bem da preservação da soberania dos Estados requerentes e requerido, ao da delegação, expressa ou tácita, da condução e direção de produção de prova oral a autoridade estrangeira, a fim de que esta proceda diretamente à inquirição da

[346] Disponível em: https://portal.stf.jus.br. Acesso em: 31 de fevereiro de 2023.

> testemunha ou do investigado, não encontra qualquer tipo de respaldo constitucional, legal ou jurisprudencial. Não por outro motivo, em caso concreto em que o Tribunal de Grande Instância de Paris (França) solicitou cooperação jurídica em matéria penal a fim de que fossem realizadas diversas diligências no Brasil, dentre elas a oitiva do investigado, a 6ª Turma do STJ reconheceu a nulidade do referido ato, porquanto todas as perguntas foram formuladas direta e exclusivamente pela autoridade judiciária francesa que acompanhava o Membro do Ministério Público Federal nomeado para realizar as diligências. O ideal é concluir, portanto, que nada impede a presença de agentes públicos estrangeiros em audiências realizadas no território nacional, conquanto não interfiram, direta ou indiretamente, na direção do referido ato processual.
>
> Noutro giro, por força da Convenção de Viena sobre Relações Diplomáticas aprovada pelo Decreto Legislativo 103/1964, e promulgada pelo Decreto nº 56.435, de 08/09/1965, Chefes de governo estrangeiro ou de Estado estrangeiro, suas famílias e membros das comitivas, embaixadores e suas famílias, funcionários estrangeiros do corpo diplomático e suas famílias, assim como funcionários de organizações internacionais em serviço (ONU, OEA, etc.) gozam de imunidade diplomática, que consiste na prerrogativa de responder no seu país de origem pelo delito praticado no Brasil.
>
> Como se percebe, por conta de tratados ou convenções que o Brasil haja firmado, ou mesmo em virtude de regras de Direito Internacional, a lei processual penal deixa de ser aplicada aos crimes praticados por tais agentes no território nacional, criando-se, assim, verdadeiro obstáculo processual à aplicação da lei processual penal brasileira.
>
> Destarte, tais pessoas não podem ser presas e nem julgadas pela autoridade do país onde exercem suas funções, seja qual for o crime praticado (CPP, art. 1º, inciso I). Em caso de falecimento de um diplomata, os membros de sua família 'continuarão no gozo dos privilégios e imunidades a que têm direito, até a expiração de um prazo razoável que lhes permita deixar o território do Estado acreditado' (art. 39, § 3º, da Convenção de Viena sobre relações diplomáticas). Admite-se renúncia expressa à garantia da imunidade pelo Estado acreditante, ou seja, aquele que envia o Chefe de Estado ou representante. Tal imunidade não é extensiva aos empregados particulares dos agentes diplomáticos.
>
> Quanto ao cônsul, este só goza de imunidade em relação aos crimes funcionais (Convenção de Viena de 1963 sobre Relações Consulares – Decreto nº 61.078, de 26/07/1967). Esse o motivo pelo qual, ao apreciar habeas corpus referente a crime de pedofilia supostamente praticado pelo Cônsul de Israel no Rio de Janeiro, posicionou-se a Suprema Corte pela inexistência de obstáculo à prisão preventiva, nos termos do art. 41 da Convenção de Viena, pois os fatos imputados ao paciente não guardavam pertinência com o desempenho das funções consulares[347].

Portanto, não há ilegalidade na utilização, em processo penal em curso no Brasil, de informações compartilhadas por força de acordo internacional de cooperação em matéria penal e oriundas de quebra de sigilo bancário determinada por autoridade estrangeira, com respaldo no ordenamento.

Dessa forma, vê-se que os princípios elencados em qualquer processo penal devem ser interpretados de forma harmoniosa; dentre eles, a liberdade de expressão e manifestação de pensamento, proteção da privacidade e dados pessoais e liberdade dos modelos negociais na internet. Essas novas tecnologias de comunicação vão além da facilitação, revestindo-se de

[347] LIMA, Renato Brasileiro. **Manual de Processo Penal** – volume único. São Paulo: Juspodiuvm, 2022, p. 84-85.

verdadeira cadeia de custódia e, como tal, traduz a história cronológica da prova, afinal, as provas digitais, embora assemelhadas aos documentos, devem ser analisadas de acordo com suas particularidades, visando sempre preservar esses direitos fundamentais indicados, além da eficiência do processo penal.

5.4 JURISPRUDÊNCIA DOS TRIBUNAIS SUPERIORES

Como já mencionado, diante de lacunas quanto à regulamentação, a jurisprudência vem se debruçando em análise a cada caso concreto.

Inicialmente, no âmbito do STF, vale destacar decisão proferida no HC 171.557/PR, julgado em 18/10/2023, versando sobre oferecimento de denúncia a operadores de mercado, com contas mantidas nas Antilhas Holandesas, visando a prática de lavagem de dinheiro, gestão fraudulenta, operação ilegal e evasão de dívidas.

O Ministério Público Federal recebeu documentos e arquivos eletrônicos relativos às contas mantidas e isso tudo em cooperação jurídica internacional, vez que as referidas contas eram controladas por residentes no Brasil. A defesa bateu pela ilicitude da prova, argumentando quebra da cadeia de custódia em razão do material digital. O STF não reconheceu tal ponto, justamente porque a evidência oriunda de cooperação jurídica internacional goza de presunção de legitimidade.

No STJ, é importante ressaltar o Agravo em Recurso Especial 1.039.417/RS, em decisão proferida em 30/04/2019, em situação em que o condenado teria armazenado e divulgado conteúdo pornográfico, utilizando softwares para outros computadores. A defesa, neste caso, sustentava violação ao princípio da integralidade da prova, como mídias sem lacre. O TRF4 afastou sinais de incorreta manipulação ou guarda (ou seja, afastou a quebra da cadeia de custódia), pois deferida a possibilidade de realizar o espelhamento, pela defesa, além de ter sido o espelhamento devidamente acompanhado por assistente técnico, sendo o material probatório devidamente manipulado e conservado.

A partir da avaliação das determinações, pode-se dizer que o debate sobre a autenticidade da cadeia de custódia da evidência digital nos órgãos judiciais mais elevados do Brasil ainda está no início.

Portanto, a ausência de uma regulamentação específica sobre a coleta, análise e utilização de evidências digitais gera grande apreensão, podendo também indicar potencial violação do direito ao processo legal[348].

No julgamento do RHC 67.379-RN, em 20/10/2016, o STJ, tratando da proteção da inviolabilidade da intimidade, entendeu que as mensagens armazenadas no aparelho estão protegidas pelo sigilo telefônico:

> Na ocorrência de atuação de crime em flagrante, ainda que seja dispensável ordem judicial para a apreensão de telefone celular, as mensagens armazenadas no aparelho estão protegidas pelo sigilo telefônico, que compreende igualmente a transmissão, recepção ou emissão de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza, por meio de telefonia fixa ou móvel ou, ainda, por meio de sistemas de informática e telemática[349].

Acerca de acesso ao Whatsapp, no RHC 99.735-SC, julgado em 27/11/2018, o STJ assim decidiu que é nula a decisão judicial que autoriza o espelhamento do Whatsapp via Código QR para acesso no Whatsapp Web, da mesma forma que são nulas todas as demais provas e atos que dela diretamente dependam ou sejam consequência, ressalvadas eventuais fontes independentes[350].

Noutro giro, no AREsp 2.309.888-MG, julgado em 17/10/2023, entendeu pela possibilidade de utilização de ações encobertas, controladas virtuais ou de agentes infiltrados no plano cibernético, inclusive via espelhamento do Whatsapp Web, desde que amparada por autorização judicial.

Acerca do código hash e a quebra da cadeia de custódia, o STJ, no julgamento do RHC 143.169-RJ, em 7/2/2023, entendeu que referida técnica obtém assinatura única para cada arquivo, daí porque sua adoção é imprescindível para validade da prova e consequentemente admissibilidade:

> [...] 4. A autoridade policial responsável pela apreensão de um computador (ou outro dispositivo de armazenamento de informações digitais) deve copiar integralmente (bit a bit) o conteúdo do dispositivo, gerando uma imagem dos dados: um arquivo que espelha e representa fielmente o conteúdo original. 5. Aplicando-se uma técnica de algoritmo hash, é possível obter uma assinatura única para cada arquivo, que teria um valor diferente caso um único bit de informação fosse alterado em alguma etapa da

---

[348] SILVEIRA, Sebastião Sérgio da. Prova Eletrônica: Novos Desafios na Busca da Verdade Real no Processo Penal. *In:* LIMA, Cíntia Rosa; SAAD-DINIZ, Eduardo.; MARRARA, Thiago (org.). **O Direito brasileiro em evolução:** estudos em homenagem à Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo. São Paulo: Almedina, 2017, p. 564.

[349] BRASIL. Superior Tribunal de Justiça. **RHC nº 67.379/RN**, Rel. Min. Ribeiro Dantas, julgado em 20/10/2016, DJe 9/11/2016.

[350] BRASIL. Superior Tribunal de Justiça. **RHC nº 99.735/SC**, Rel. Min. Laurita Vaz, julgado em 27/11/2018, DJe 12/12/2018.

> investigação, quando a fonte de prova já estivesse sob a custódia da polícia. Comparando as hashes calculadas nos momentos da coleta e da perícia (ou de sua repetição em juízo), é possível detectar se o conteúdo extraído do dispositivo foi modificado. 6. É ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia. No processo penal, a atividade do Estado é o objeto do controle de legalidade, e não o parâmetro do controle, isto é, cabe ao Judiciário controlar a atuação do Estado-acusação a partir do direito, e não a partir de uma autoproclamada confiança que o Estado-acusação deposita em si mesmo. 7. No caso dos autos, a polícia não documentou nenhum dos atos por ela praticados na arrecadação, armazenamento e análise dos computadores apreendidos durante o inquérito, nem se preocupou em apresentar garantias de que seu conteúdo permaneceu íntegro enquanto esteve sob a custódia policial. Como consequência, não há como assegurar que os dados informáticos periciados são íntegros aos que existiam nos computadores do réu. 8. Pela quebra da cadeia de custódia, são inadmissíveis as provas extraídas dos computadores do acusado, bem como as provas delas derivadas, em aplicação analógica do art. 157, § 1º, do CPP[351].

Ainda acerca do acesso ao celular, a Quinta Turma do Superior Tribunal de Justiça, por unanimidade, no julgamento do AgRg no Habeas Corpus nº 828054, de relatoria do Ministro Joel Ilan Paciornik, julgado em 23/04/2024, decidiu que são inadmissíveis no processo penal as provas obtidas de celular quando não forem adotados procedimentos para assegurar a idoneidade e a integridade dos dados extraídos. Nesse sentido:

> PROCESSUAL PENAL. AGRAVO REGIMENTAL NO HABEAS CORPUS. TRÁFICO DE DROGAS. APREENSÃO DE CELULAR. EXTRAÇÃO DE DADOS. CAPTURA DE TELAS. QUEBRA DA CADEIA DE CUSTÓDIA. INADMISSIBILIDADE DA PROVA DIGITAL. AGRAVO REGIMENTAL PROVIDO.
> 1. O instituto da cadeia de custódia visa a garantir que o tratamento dos elementos probatórios, desde sua arrecadação até a análise pela autoridade judicial, seja idôneo e livre de qualquer interferência que possa macular a confiabilidade da prova.
> 2. Diante da volatilidade dos dados telemáticos e da maior suscetibilidade a alterações, imprescindível se faz a adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios que assegurem a preservação integral dos vestígios probatórios, de forma que seja possível a constatação de eventuais alterações, internacionais ou não, dos elementos inicialmente coletados, demonstrando-se a higidez do caminho percorrido pelo material.
> 3. A auditabilidade, a repetibilidade, a reprodutibilidade e a justificatibilidade são quatro aspectos essenciais das evidências digitais, os quais buscam ser garantidos pela utilização de metodologias e procedimentos certificados, como, e.g., os recomendados pela ABNT.
> 4. A observação do princípio da mesmidade visa 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 dados do arquivo digital.

[351] BRASIL. Superior Tribunal de Justiça. **AgRg no RHC nº 143.169/RJ**, Rel. Min. Messod Azulay Neto, Rel. para acórdão Min. Ribeiro Dantas, Quinta Turma, julgado em 7/2/2023, DJe 2/3/2023.

> 5. De relevo trazer à baila o entendimento majoritário desta Quinta Turma no sentido de que "é ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia" (AgRg no RHC n. 143.169/RJ, relator Ministro Messod Azulay Neto, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, DJe de 2/3/2023).
> 6. Neste caso, não houve a adoção de procedimentos que assegurassem a idoneidade e a integridade dos elementos obtidos pela extração dos dados do celular apreendido. Logo, evidentes o prejuízo causado pela quebra da cadeia de custódia e a imprestabilidade da prova digital[352].

Em casos de *ramsonware* – extorsão digital – e competência, o STJ entendeu que é suficiente a ocorrência de uma das situações previstas no inciso IV do art. 109 da CF, para determinar a competência da Justiça Federal:

> [...] 3. Em se tratando de crime previsto em tratado ou convenção internacional, a competência da Justiça Federal é firmada "quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente" (art. 109, V, da Constituição da República), ou se for praticado "em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas", nos termos do inciso IV, do mesmo dispositivo constitucional. Basta a presença de uma dessas hipóteses para que seja firmada a competência da Justiça Federal, não sendo necessária a presença concomitante de ambas, como entendeu o Juízo Suscitante [...]
> 6. No caso, ao contrário do afirmado pelo Juízo Suscitante, há prova da internacionalidade do delito, pois as investigações feitas pela autoridade policial constataram que tanto o registro como o acesso a ao menos um dos e-mails utilizados pelo criminoso, para a prática do delito, foram feitos no estrangeiro. 7. Firmada a competência da Justiça Federal, nos termos do art. 109, inciso V, da Constituição da República [...][353].

Aqui, vê-se a importância da jurisprudência para suprir os *gaps* que ainda remanescem, notadamente quanto à prova digital, à guisa de ausência de diploma específico quanto à sua utilização.

Vê-se que as decisões tratam especialmente dos meios de obtenção da prova digital e, também, com o enfrentamento da questão da preservação dos direitos fundamentais.

---

[352] BRASIL. Superior Tribunal de Justiça. **AgRg no HC nº 828.054**, Rel. Min. Joel Ilan Paciornik, julgado em 23/04/2024, DJe 29/04/2024.
[353] BRASIL. Superior Tribunal de Justiça. **CC n. 197.032/AM**, Rel. Min. Laurita Vaz, Terceira Seção, julgado em 14/06/2023, DJe 21/06/2023.

CONCLUSÃO

No processo penal, cabe ao julgador avaliar as evidências coletadas e, com base nos argumentos apresentados pelas partes, aplicar a legislação ao caso concreto. Isso destaca a relevância das provas, permitindo que o magistrado receba uma quantidade significativa de informações que auxiliem na recriação de um fato criminoso específico.

A finalidade da prova é, portanto, reconstituir os eventos analisados no procedimento e procurar a máxima convergência com a realidade histórica, ou seja, com a veracidade dos acontecimentos, buscando o maior grau de proximidade em relação a como ocorreram os fatos no tempo e espaço.

Diante de todo esse contexto, torna-se evidente a relevância da análise da prova e suas diversas consequências. E, nesse aspecto, a prova digital assume um papel fundamental atualmente, em virtude das novas tecnologias que otimizaram a coleta, o armazenamento, a avaliação e a disseminação de informações.

Dadas as particularidades das provas digitais, seu exame, relativamente recente em constante desenvolvimento, exige, na prática, atenção em relação às garantias individuais que foram arduamente conquistadas e que não devem ser ignoradas sob a justificativa de se procurar uma solução em um processo a todo e qualquer custo.

Dessa forma, é imprescindível que o sistema jurídico se adapte para garantir a proteção dos direitos fundamentais e, ao mesmo tempo, confira a devida punição àquele que infringiu o ordenamento jurídico.

Hoje, com a internet fazendo parte do próprio indivíduo (afinal, não se olvida que quase a totalidade das atividades, não apenas pessoais, mas também profissionais, são realizadas por meio do computador/smartphones), há evidente ambiente de informações excessivas dos indivíduos e, por tal razão, na investigação, é crucial que os dados pessoais não sejam utilizados de forma que fira o ordenamento jurídico, tampouco de fomo antiético.

O papel do direito é, essencialmente, regular as interações sociais, assegurando que os membros dessa sociedade tenham responsabilidade e sejam também protegidos.

Assim, o que se vê, hoje, é cenário no qual a prova digital está inserida dentro da nossa realidade, porém, ainda sem normativas que tutelem de forma completa, daí porque cabe à jurisprudência fazer a análise, considerando cada caso concreto.

É fato: o legislador não consegue acompanhar as mudanças tecnológicas – ao menos não na velocidade como ocorrem na prática.

Além disso, no contexto empresarial, é igualmente crucial estabelecer um sistema de segurança, especialmente no que se refere à criminalidade econômica, por exemplo, que frequentemente impacta não apenas o estado nacional, mas também outras nações. Tudo isso demanda a implementação de medidas que sejam compartilhadas e reconhecidas internacionalmente.

É fundamental, portanto, reavaliar – ponderando e reconsiderando – alguns fundamentos do processo penal.

O direito – especialmente no que diz respeito às provas – está evoluindo de maneira surpreendente. Assim, é necessário repensar a maneira como as evidências – em especial as digitais – são coletadas, garantindo sua efetividade sem olvidar os direitos e garantias já consagrados.

Não se pretendeu, por óbvio, esgotar o tema, trazendo todas as variáveis possíveis para solução, mas destacar pontos que merecem ser observados e, a partir de então, criar novos raciocínios e ferramentas.

Assim, a criação de um processo penal digital ou a inserção de normas específicas que tratem da prova digital é necessária. Afinal, não se pode trabalhar com as mesmas ferramentas ordinárias diante dessa nova era. Existem mudanças, com pontos evidentes que demarcam a passagem analógico-digital e, a ausência de tratamento específico pode gerar insegurança jurídica e/ou invalidação da prova, o que não se pode admitir.

De todo modo, é certo que o diploma ou dispositivo que verse sobre o tema, deverá ser dotado de conceitos abertos, justamente em razão das constantes mudanças tecnológicas, por isso deve haver todo um cuidado, evitando qualquer retrocesso ou normas cuja ineficácia seja evidente.

Em outras palavras, a modernização do direito processual penal deverá estar alinhada aos deságios da era digital, com a concretização de um sistema de justiça mais eficiente, capaz de lidar com a complexidade do mundo contemporâneo, sem, no entanto, comprometer as liberdades individuais.

A ideia é a criação de um modelo que encontre consonância com aquele já previsto, consideradas as características das provas digitais, notadamente as questões empresariais e transnacionais, visando celeridade e, ao mesmo tempo, proteção e garantia aos direitos fundamentais.

REFERÊNCIAS

ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital:** Doutrina e Prática em Debate. v. 2. São Paulo. Internet Lab, 2019.

ARAS, Vladimir; LUZ, Ilana M. **Lavagem de dinheiro: comentários à Lei n. 9.613/1998**. São Paulo: Almedina, 2023. *E-book.* ISBN 9786556279152. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556279152/.

ARAÚJO, Janaína. Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos. **Rádio Senado,** 29 mar. 2023. Disponível em https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos#:~:text=Conhecida%20como%20Lei%20Carolina%20Dieckmann%2C%20a%20norma%20ganhou%20vida%20a,ceder%20%C3%A0%20extors%C3%A3o%20dos%20criminosos. Acesso em: 31 de out. 2024.

AUGUSTO, Victor; VALENTE, Estevam. **Inteligência artificial e o Direito Penal:** o propósito da responsabilidade criminal em decorrência de sistemas tecnológicos altamente complexos nas empresas. Belo Horizonte, São Paulo: D'Plácido, 2023.

BADARÓ, Gustavo Henrique Righi Ivahy. **Ônus da prova no processo penal.** São Paulo: Editora Revista dos Tribunais, 2003.

BADARÓ, Gustavo. A cadeia de custódia e sua relevância para a prova penal. *In:* SIDI, Ricardo; LOPES, Anderson B. (org.). **Temas atuais da investigação preliminar no processo penal**. Belo Horizonte: D'Plácido, 2018.

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM,** ano 29, n. 343, jun. p. 7-9, 2021. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325/627. Acesso em: 31 out. 2024.

BADARÓ, Gustavo Henrique. **Processo Penal**.11. ed., São Paulo: Thomson Reuters Brasil, 2023.

BADARÓ, Gustavo Henrique. **Epistemologia Judiciária e Prova Penal**. 2. ed., São Paulo: Thomson Reuters, 2023.

BARBAS, Leandro Moreira Valente; DEVEIKIS, Gabriel Druda. O compliance como "autorregulação regulada" e desafios técnicos de ordem prática. **Migalhas,** 9 abr. 2021. Disponível em https://www.migalhas.com.br/depeso/340170/o-compliance-como-autorregulacao-regulada. Acesso em: 01 jul. 2023.

BARRETO, Alesandro Gonçalves; SANTOS, Hericson dos. **Deep Web:** Investigação no submundo da internet. Rio de Janeiro: Brasport, 2019.

BARRETO, Leonardo; ALVES, Moreira. **Processo Penal Parte Geral**. 10. ed. Salvador: Juspodivm, 2020.

BARRILARI, Claudia Cristina. **Crime empresarial, autorregulação e compliance.** 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

BARROS, Guilherme Freire de Melo. **Estatuto da Criança e do Adolescente.** 14. ed. Salvador: Juspodivm, 2020.

BARROS, Rafael. Entenda a teoria do direito penal do inimigo no Brasil. **Aurum**, 12 jun. 2023. Disponível em: https://www.aurum.com.br/blog/direito-penal-do-inimigo/. Acesso em 12 out. 2024.

BELANDI, Caio. 161,6 milhões de pessoas com 10 anos ou mais de idade utilizaram a Internet no país, em 2022. **AGÊNCIA IBGE**, 09 nov. 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=Para%2066%2C1%25%20dos%20idosos,2021%20(84%2C4%25. Acesso em: 03 mar. 2024.

BERTOCELLI, Rodrigo de Punho. Compliance. *In:* CARVALHO, André Castro; ALVIM, Tiago Cripa; VENTURINI, Rodrigo Bertoccell (cood.). **Manual de Compliance.** 2. ed. Rio de Janeiro: Forense, 2020.

BIFFE JÚNIOR, João; LEITÃO JÚNIOR, Joaquim**.** O acesso pela polícia a conversas gravadas no Whatsapp e as gerações probatórias decorrentes das limitações à atuação estatal. **Genjurídico**, 12 ago. 2016. Disponível em: https://blog.grupogen.com.br/juridico/areas-de-interesse/penal/o-acesso-pela-policia-a-conversas-gravadas-no-whatsapp-e-as-geracoes-probatorias-decorrentes-das-limitacoes-a-atuacao-estatal/. Acesso em: 06 jun. 2024.

BOMFATI, Cláudio Adriano; KOLBE, Armando Júnior. **Crimes cibernéticos**. Curibita: Intersaberes, 2020.

BRASIL. **Decreto-lei 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, dezembro 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 20 ago. 2024.

BRASIL. **Decreto-lei 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Brasília, outubro 1941. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-3689-3-outubro-1941-322206-publicacaooriginal-1-pe.html. Acesso em: 20 ago. 2024.

BRASIL. [Constituição 1988]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 27 abr. 2024.

BRASIL. **Lei 12.850/13.** Define organização criminosa. Brasília, agosto 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.htm. Acesso em: 20 ago. 2024.

BRASIL. **Lei 9.295/96.** Lei das interceptações telefônicas. Brasília, julho 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L9295.htm#:~:text=LEI%20N%C2%BA%209.295%2C%20DE%2019%20DE%20JULHO%20DE%201996.&text=Disp%C3%B5e%20sobre%20os%20servi%C3%A7os%20de,regulador%20e%20d%C3%A1%20outras%20provid%C3%AAncias. Acesso em: 20 ago. 2024.

BRASIL. **Lei 12.965/14**. Marco Civil da Internet. Brasília, abril 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 ago. 2024.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso em Habeas Corpus nº 51531** – RO, 2014. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=59034141&num_registro=201402323677&data=20160509&tipo=3&formato=PDF. Acesso em: 11 jun. 2024.

BRASIL. **Lei nº 13.105, de 16 de março de 2015.** Código de Processo Civil. Brasília, março 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 20 ago. 2024.

BRASIL. Superior Tribunal de Justiça. **RHC nº 67.379/RN**, Rel. Min. Ribeiro Dantas, julgado em 20/10/2016, DJe 9/11/2016.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso em Mandado de Segurança Nº55.019-DF. 2017.** Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1667238&num_registro=201702013432&data=20180201&formato=PDF. Acesso em: 10 ago. 2024.

BRASIL. Superior Tribunal de Justiça. **RHC nº 99.735/SC,** Rel. Min. Laurita Vaz, julgado em 27/11/2018, DJe 12/12/2018.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados (LGDP). Brasília, agosto 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 ago. 2024.

BRASIL, **Projeto de Lei 10.372, de 06 de junho de 2018.** Introduz modificações na legislação penal e processual penal para aperfeiçoar o combate ao crime organizado, aos delitos de tráfico de drogas [...]. Câmara dos Deputados. Brasília, junho 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2178170&fichaAmigavel=nao. Acesso em: 10 out. 2024.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 10.372**, de 06 de junho de 2018. Introduz modificações na legislação penal e processual penal para aperfeiçoar o combate ao crime organizado [...]. Brasília, 2018. Disponível em:https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1666497&filename=PL%2010372/2018. Acesso em: 05 ago. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. **Manual de Cooperação Jurídica Internacional: Matéria Penal e Recuperação de Ativos**. 4. ed., 2019. Disponível em https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagem-de-dinheiro/drci/publicacoes/manuais/cooperacao-juridica-internacional-em-materia-penal/manual-penal-online-final-2.pdf. Acesso em: 11 jul. 2024.

BRASIL, **PL 5.441/2020.** Define os crimes cibernéticos e dá outras providências. Câmara dos Deputados. Brasília, dezembro 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2266423ra.leg.br). Acesso em: 3 abr. 2024.

BRASIL. **Projeto de Lei nº 4939/20, de 15 de outubro de 2020**. CÂMARA DOS DEPUTADOS. Comissão de Juristas. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2264367#:~:text=PL%204939%2F2020%20Inteiro%20teor,Projeto%20de%20Lei&text=Disp%C3%B5e%20sobre%20as%20diretrizes%20do,7%20de%20dezembro%20de%201940. Acesso em: 3 de janeiro de 2023.

BRASIL. Superior Tribunal de Justiça. **REsp 1.568.445/PR**, relator Ministro Rogério Schietti Cruz, relator para acórdão Ministro Ribeiro Dantas, Terceira Seção, julgado em 24/6/2020, DJe de 20/8/2020.

BRASIL. Superior Tribunal de Justiça. **RMS 61302** / RJ, Relator Ministro Rogerio Schietti Cruz, Terceira Seção, julgado em 26/08/2020, DJe 04/09/2020. RMPRJ, vol. 78, p. 483.

BRASIL. PL 4.939/20. Dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências. Brasília, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node08pwjhswz835euh8tzvacb7on17491799.node0?codteor=1936366&filename=PL+4939/2020. Acesso em: 10 out. 2024.

BRASIL. Supremo Tribunal Federal. **ADI 6529/DF**, Rel. Min. Cármen Lúcia, julgamento virtual finalizado em 8/10/2021.

BRASIL. Superior Tribunal de Justiça. **RMS nº 66.392**/RS (2021/0134439-7), Relator Ministro João Otávio de Noronha. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202101344397&dt_publicacao=19/08/2022. Acesso em: 24 out. 2024.

BRASIL. Supremo Tribunal Federal. **ADI 4.906/DF**, Rel. Min. Nunes Marques, Tribunal Pleno, julgado em 11/09/2024, publicado em: DJe-s/n, 24/10/2024. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%204906%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em: 07 out. 2024.

BRASIL. **Decreto 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro

de 2001. Presidência da República, abril 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm#:~:text=DECRETO%20N%C2%BA%2011.491%2C%20DE%2012,23%20de%20novembro%20de%202001. Acesso em: 10 ago. 2024.

BRASIL. Superior Tribunal de Justiça. **CC n. 197.032/AM**, Rel. Min. Laurita Vaz, Terceira Seção, julgado em 14/06/2023, DJe 21/06/2023.

BRASIL. Superior Tribunal de Justiça. **AgRg no RHC nº 143.169/RJ**, Rel. Min. Messod Azulay Neto, Rel. para acórdão Min. Ribeiro Dantas, Quinta Turma, julgado em 7/2/2023, DJe 2/3/2023.

BRASIL. Supremo Tribunal Federal. **ADI 6.298/DF, ADI 6.299/DF, ADI 6.300/DF e ADI 6.305/DF**, Rel. Min. Luiz Fux, julgados em 24/08/2023.

BRASIL. Superior Tribunal de Justiça. **REsp nº 2.139.749/SP** (2023/0068660-0), Relator Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 27/08/2024, DJe 30/08/2024.

BRASIL. Superior Tribunal de Justiça. **AgRg no AREsp nº 2.218.334**/MG, Rel. Min. Reynaldo Soares da Fonseca, Quinta Turma, julgado em 16/4/2024, DJe 23/4/2024.

BRASIL. Superior Tribunal de Justiça. **AgRg no HC nº 828.054/RN**, Rel. Min. Joel Ilan Paciornik, julgado em 23/4/2024. Disponível em https://processo.stj.jus.br/SCON/pesquisar.jsp?pesquisaAmigavel=+%3Cb%3EHC+828.054%3C%2Fb%3E&b=ACOR&tp=T&numDocsPagina=10&i=1&O=&ref=&processo=&ementa=&nota=&filtroPorNota=&orgao=&relator=&uf=&classe=&juizo=&data=&dtpb=&dtde=&operador=e&thesaurus=JURIDICO&p=true&livre=HC+828.054. Acesso em 27 jul. 2024.

BRASIL. Superior Tribunal de Justiça. **AgRg no HC nº 828.054**, Rel. Min. Joel Ilan Paciornik, julgado em 23/04/2024, DJe 29/04/2024.

CANÁRIO, Pedro. Cooperação jurídica com EUA para quebra de sigilo telemático fracassa 77% das vezes. **ConJur,** 8 mar. 2018. Disponível em: https://www.conjur.com.br/2018-mar-08/cooperacao-eua-quebra-sigilo-fracassa-77-vezes/#:~:text=O%20Mlat%20(Acordo%20de%20Assist%C3%AAncia,ao%20governo%20dos%20Estados%20Unidos. Acesso em: 03 maio 2024.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins de; PINHO, Vinícius. ***Compliance* 60º:** Riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CAPEZ, Fernando. **Curso de Processo Penal.** 5. edição. Saraiva: São Paulo, 2006.

CAPEZ, Fernando. **Legislação Penal Especial.** 18. ed. São Paulo: Saraivajur, 2023.

CAPEZ, Fernando. Uso de prova ilícita para evitar que um inocente seja condenado. **ConJur,** 24 ago. 2023. Disponível em: https://www.conjur.com.br/2023-ago-24/controversias-juridicas-provas-ilicitas-inocencia/. Acesso em: 1 fev. 2024.

CAVALCANTE, Márcio André Lopes. São ilegais as provas obtidas por policial militar que, designado para coletar dados nas ruas como agente de inteligência, passa a atuar, sem autorização judicial, como agente infiltrado em grupo criminoso. **Buscador Dizer o Direito.** Manaus. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/5fde40544cff0001484ecae2466ce96e#:~:text=por%20tempo%20limitado.-,S%C3%A3o%20ilegais%20as%20provas%20obtidas%20por%20policial%20militar%20que%2C%20designado,agente%20infiltrado%20em%20grupo%20criminoso. Acesso em 20 de julho de 2024.

CAVALCANTE, Márcio André Lopes. Não é possível a quebra de sigilo de dados informáticos estáticos (registros de geolocalização) nos casos em que haja a possibilidade de violação da intimidade e vida privada de pessoas não diretamente relacionadas à investigação criminal. **Buscador Dizer o Direito,** Manaus. Disponível em: https://buscadordizerodireito.com.br/jurisprudencia/detalhes/35ec253885cf090f80881b44180afb00. Acesso em: 12 out. 2024.

CAVALCANTE, Márcio André Lopes. São constitucionais os arts. 13-A e 13-B do CPP, inseridos pela Lei 13.344/2016**. Buscador Dizer o Direito**, Manaus. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/8e86a13d18f6dcab5a77f0a4525c0b20. Acesso em: 18 out. 2024.

CAVALCANTE, Márcio André Lopes. São nulas as provas obtidas a partir de dados preservados em contas da internet (com o congelamento e a consequente perda da disponibilidade), mediante requerimento do Ministério Público, sem a prévia autorização judicial de quebra de sigilo e fora das hipóteses legais**. Buscador Dizer o Direito**, Manaus. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/0dd4f2526c7c874d06f19523264f6552. Acesso em: 23 out. 2024.

CAVALCANTE, Márcio André Lopes. Facebook Inc, mesmo estando situada nos EUA, deve cumprir ordens judiciais para fornecimento de dados independentemente de pedido de cooperação jurídica internacional**. Buscador Dizer o Direito**, Manaus. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/8eab914c88e95773ea769310350ad7cb. Acesso em: 24 out. 2024.

CASTRO, E. L. de F.; WINTER, P. P. O conflito de jurisdições em caso de violação de direitos da personalidade por publicação na internet. **Revista de Estudos Jurídicos da UNESP**, Franca, v. 18, n. 28, 2015.

COSTA, Klaus Negri; ARAÚJO, Fábio Roque. **Processo Penal Didático**. 3. ed. Salvador: Juspodivm, 2020.

COURA, Kalleo; LEORATTI, Alexandre**.** Juízes ordenam quebra de sigilo de sigilo com base em localização. **Jota,** 27 maio 2019. Disponível em: https://www.jota.info/especiais/juizes-ordenam-quebra-coletiva-de-sigilo-de-dados-com-base-em-localizacao 27052019. Acesso em: 7 jul. 2024.

DIZER O DIREITO. O vazamento de dados pessoais não gera dano moral presumido. **Dizer o Direito,** 31 mar. 2023. Disponível em: https://www.dizerodireito.com.br/2023/03/o-vazamento-de-dados-pessoais-nao-gera.html. Acesso em: 24 out. 2024.

DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schreiner**.** Obtenção de provas digitais e jurisdição na internet. **Crimes Cibernéticos: Coletânea de Artigos**. Ministério Público Federal. v. 3, 2018.

DUARTE, David; MEALHA, Tiago. **Introdução à deep web**. Lisboa: IET Working Papers Series, 2016.

FERNANDES, Robério Fernandes Júnior. A evolução e o impacto das gerações probatórias na persecução penal sob os influxos dos atuais mecanismos telefônicos. **Escola superior do Ministério Público do Ceará**, ano 14, n. 1, jan.-jul., p. 11-30, 2022. Disponível em: https://revistaacademica.mpce.mp.br/revista/article/view/202/167. Acesso em: 27 out. 2024.

FILARDI, Rosemaria Adalardo; SOUZA, Damares Pereira de. Programas de compliance como autorregulação. **DIGE – Direito Internacional e Globalização Econômica,** v. 2 n. 02, p. 46-59, 2023. Disponível em: https://revistas.pucsp.br/index.php/DIGE/article/view/64290. Acesso em: 08 ago. 2024.

FRANCO, Isabel. **Guia Prático de Compliance**. Rio de Janeiro: Forense, 2019. *E-book.* ISBN 9788530988692. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530988692/. Acesso em: 01 nov. 2024.

GLEIZE, Orlandino. Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal. **Jota,** 31 jul. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-31072019. Acesso em: 20 ago. 2024.

GUIMARÃES, José Leite Júnior. **Responsabilidade Penal das pessoas jurídicas nos crimes econômicos** – Sociedade de risco e empresa. São Paulo: Dialética, 2023.

IBGC. **Código das melhores práticas de governança corporativa**. 6. ed., 2023, p. 17. Disponível em https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/24640/2023_C%c3%b3digo%20das%20Melhores%20Pr%c3%a1ticas%20de%20Governan%c3%a7a%20Corporativa_6a%20Edi%c3%a7%c3%a3o.pdf. Acesso em: 22 out. 2024.

INFOMONEY. Metaverso: tudo sobre o mundo virtual que está chamando a atenção dos investidores. **Infomoney,** 8 nov. 2022. Disponível em https://www.infomoney.com.br/guias/metaverso/. Acesso em: 1 nov. 2024.

INTERNET RIGHTS AND PRINCIPLES DYNAMIC COALITION. Promoting human rights as digital rights. **IRPC,** 19 jun. 2024. Disponível em https://internetrightsandprinciples.org/. Acesso em: 12 out. 2024.

JONES, Franklin. **Rastreando a verdade.** A cadeia de custódia da prova. Maringá: Viseu, 2023**.**

KIST, Dario José. **Prova Digital no Processo penal**. Leme, SP: JH Mizuno, 2019.

KMPG. Conselho de Administração: Prioridades para a agenda de 2024. **KMPG.** Disponível em: https://assets.kpmg.com/content/dam/kpmg/br/pdf/2024/03/Conselho-de-Administracao-Prioridades-para-a-agenda-de-2024.pdf. Acesso em: 20 out. 2024.

KNIJNIK, Danilo. A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI. **Revista da Escola da Magistratura do TRF da 4ª Região**, ano 2, número 4. Porto Alegre/RS, 2016. Disponível em: https://www.trf4.jus.br/trf4/upload/editor/2019/bnu_05-a-trilogia.pdf. Acesso em: 4 jun. 2024.

LAW, Thomas. **A Lei Geral de Proteção de Dados – LGPD.** Uma análise comparada ao novo modelo chinês. São Paulo: D'Plácido, 2021.

LIMA, Renato Brasileiro. **Pacote Anticrime.** Comentários à Lei 13.964/2019. Salvador: Juspodivm, 2020.

LIMA, Renato Brasileiro. **Manual de Processo Penal** – volume único. São Paulo: Juspodivm, 2022.

LOPES Júnior, Aury. **Direito Processual Penal**. 21. edição. São Paulo: Saraivajur, 2024.

LÓSSIO, Claudio Joel B. **Proteção de dados e compliance digital**. 2. ed. São Paulo: Almedina, 2023. *E-book.* ISBN 9786556279893. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556279893/. Acesso em: 01 nov. 2024.

MAGRAMO, Kathleen. Golpistas usam deepfake de diretor financeiro e roubam US$ 25 milhões. **CNN Brasil**, 05 fev. 2024. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/golpistas-usam-deepfake-de-diretor-financeiro-e-roubam-us-25-milhoes/. Acesso em: 31 de out. 2024.

MARTINS, Amanda Cunha e Mello Smith. **Transferência internacional de dados pessoais**. Belo Horizonte-São Paulo: D'Plácido, 2022.

MORAES, Alexandre de. **Direito Constitucional**. 40. ed. Rio de Janeiro: Atlas, 2024. *E-book.* p.92. ISBN 9786559776375. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559776375/. Acesso em: 18 out. 2024.

MOTTA, Sylvio. **Direito Constitucional.** 29. ed. Rio de Janeiro: Método, 2021, *E-Book*, p. 230, ISBN 9788530993993. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530993993/. Acesso em: 18 out. 2024.

MOUGENOT, Edilson. **Curso de processo penal**. 13. ed. São Paulo: Saraiva Educação, 2019.

MOUGENOT, Edilson. **Curso de processo penal**. 14. ed. São Paulo: Saraiva Jur, 2024.

MOURA, Grégore Moreira de. **Curso de Direito Penal Informático**. Belo Horizonte, São Paulo: D'Plácido, 2021.

NATIONAL CONSTITUTION CENTER. **Fourth Amendment:** Search and Seizure. Disponível em: https://constitutioncenter.org/the-constitution/amendments/amendment-iv. Acesso em: 11 jun. 2024.

NERY, Carmen. Em 2023, 88,0% das pessoas com 10 anos ou mais utilizaram Internet. **AGÊNCIA IBGE,** 16 ago. 2024. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet. Acesso em: 31 out. 2024.

NUCCI, Guilherme de Souza. **Princípios constitucionais penais e processuais penais**. 4. ed. Rio de Janeiro: Forense, 2015.

NUCCI, Guilherme de Souza. **Curso de direito processual penal.** 17. ed. Rio de Janeiro: Forense, 2020.

NUCCI, Guilherme de Souza. **Manual de Processo Penal** – Volume Único. 5. ed. Rio de Janeiro: Forense, 2024.

NUNES, Vinícius. Moraes vota a favor de quebra de sigilo de dados de pessoas indeterminadas. **Jota,** 16 out. 2024. Disponível em: https://www.jota.info/stf/do-supremo/moraes-vota-a-favor-de-quebra-de-sigilo-de-dados-de-pessoas-indeterminadas. Acesso em: 19 out. 2024.

OLIVEIRA, Vinícius Machado de. ABNT NBR ISO/IEC 27037:2013. **Academia Forense Digital.** Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/. Acesso em: 8 out. 2024.

ORWELLIANA. *In:* **PRIBERAM**, Dicionário Priberam da Língua Portuguesa. Disponível em: https://dicionario.priberam.org/orwelliana. Acesso em: 10 jul. 2024.

PACELLI, Eugênio. **Curso de processo penal**. 28. edição. Lumen Juris: Rio de Janeiro, 2024.

PIGATIN, Erika. Crimes Cibernéticos. **JusBrasil,** 2019. Disponível em https://www.jusbrasil.com.br/artigos/crimes-ciberneticos/747423400?_gl=1*iiruz6*_gcl_aw*R0NMLjE3MjU5MDE0NTUuQ2p3S0NBand1ZnEyQmhBbUVpd0FuWnF3OHZwRE1ZbTlkc1p1aDQ3OXItRmdJNXJhUVdSdUxnVXItS0UyU0lmZUlHelNXLTJaeEpsMnRSb0NwMXNRQXZEX0J3RQ..*_gcl_au*MjgzMTc2MzM3LjE3MjIyNjU2MjM.*_ga*MTM3ODY2ODEzLjE2NjU3NDA3MzE.*_ga_QCSXBQ8XPZ*MTcyODQwMzM5MC4xODcuMC4xNzI4NDAzMzkwLjYwLjAuMA. Acesso em: 09 out. 2024.

POLÍCIA FEDERAL. Acordo de Cooperação Internacional. **Ministério da Justiça e Segurança Pública.** Disponível em https://www.gov.br/pf/pt-br/assuntos/acordos-de-cooperacao#:~:text=Pol%C3%ADcia%20Federal%20se%20utiliza%20da,a%20coopera%C3%A7%C3%A3o%20e%20assist%C3%AAncia%20m%C3%BAtuas. Acesso em: 11 out. 2024.

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

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

PROVA. *In:* **DICIO**, Dicionário Online de Português. Porto: 7Graus, 2024. Disponível em: https://www.dicio.com.br/prova. Acesso em: 10 abr. 2023.

RIZZO, Maria Balbina M. **Prevenção da lavagem de dinheiro nas organizações**. 2. ed. São Paulo: Trevisan Editora, 2016. *E-book.* ISBN 9788599519875. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788599519875/.

ROSA, Alexandre Morais da. **Guia compacto do processo penal conforme a teoria dos jogos.** 3. ed. Florianópolis: Empório do Direito, 2016.

SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda uma disciplina própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. **Rev. Bras. de Direito Processual Penal,** Porto alegre, v. 10, n. 3, e1071, set-dez. 2024. Disponível em https://revista.ibraspp.com.br/RBDPP/article/view/1071/547. Acesso em: 31 out. 2024.

SALEME, Edson R. **Direito constitucional**. 5. ed. Barueri: Manole, 2022. *E-book.* p.137. ISBN 9786555766370. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555766370/. Acesso em: 07 jun. 2024.

SANTOS, Fábio Antônio Tavares dos. **Direito Penal Empresarial** – a responsabilidade penal horizontal. São Paulo: LiberArs, 2022.

SILVA, Lilian Reis da. Benefícios do compliance e da gestão de riscos. **Núcleo do Conhecimento,** 13 dez. 2021. Disponível em https://www.nucleodoconhecimento.com.br/administracao/beneficios-do-compliance. Acesso em: 23 out. 2024.

SILVA, Virgílio Afonso da. **A constitucionalização do direito** – os direitos fundamentais nas relações entre particulares. São Paulo: Editora Malheiros, 2011.

SILVEIRA, Sebastião Sérgio da. Prova Eletrônica: Novos Desafios na Busca da Verdade Real no Processo Penal. *In:* LIMA, Cíntia Rosa; SAAD-DINIZ, Eduardo.; MARRARA, Thiago (org.). **O Direito brasileiro em evolução**: estudos em homenagem à Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo. São Paulo: Almedina, 2017.

SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. 2. edição. São Paulo: Revista dos Tribunais, 2024.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco Civil da Internet**: construção e aplicação. Juiz de Fora: Editar Editora Associada, 2016.

STJ. **Cooperação Jurídica Internacional.** Disponível em https://international.stj.jus.br/pt/Cooperacao-Internacional/Cooperacao-Juridica-Internacional. Acesso em: 10 out. 2024.

STF NOTÍCIAS. STF autoriza retorno imediato do X e determina que Anatel adote providências para retomada do serviço. **STF Notícias,** 8 out. 2024. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-autoriza-o-retorno-imediato-do-x-e-determina-que-anatel-adote-providencias-para-a-retomada-do-servico/. Acesso em: 11 out. 2024.

TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 5. ed. São Paulo: Saraiva, 2020. E-book.

TEIXEIRA, Tarcísio. **Direito Digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024.

UNIÃO EUROPEIA. Legislação - **Jornal Oficial da União Europeia**, 4 maio 2016. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN. Acesso em: 10 out. 2024.

UNIÃO EUROPEIA. DIRETIVA (UE) 2016/ 680 DO PARLAMENTO EUROPEU E DO CONSELHO - de 27 de abril de 2016 - relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/ 977/ JAI do Conselho (europa.eu), disponível em https://eur-lex,europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HR. Acesso em: 13 jan. 2023.

VALENTE, Manuel Monteiro Guedes. **Cadeia de Custódia da Prova**. 4. ed. Coimbra: Almedina, 2023.

VALENTE, Manuel Monteiro. Os Direitos e Garantias dos cidadãos investigados na era digital. *In:*ANTONIALLI, Dennys; FRAGOSO, Nathalie (ed.). **Direitos Fundamentais e Processo Penal na Era Digital.** Doutrina e prática em debate, vol. 2., São Paulo: 2019, InternetLab, p. 24-45.

VAZ, Denise Provasi. **Provas Digitais no Processo Penal:** Formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade de São Paulo, São Paulo, 2012.

WENDT, Emerson. **Crimes Cibernéticos:** ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013.

WENDT, Emerson; Jorge, Higor Vinícius Nogueira. **Crimes Cibernéticos:** ameaças e procedimentos de investigação. 3. ed. Rio de Janeiro: Brasport, 2021.