FADISP

REVISTA PENSAMENTO JURÍDICO
ISSN 2238944-X

CRIMES DIGITAIS, PROVAS DIGITAIS E POLÍTICA PÚBLICA DE PERSECUÇÃO PENAL NO BRASIL: UMA REALIDADE INCÔMODA

DIGITAL CRIMES, DIGITAL EVIDENCE AND PUBLIC POLICY OF CRIMINAL PERSECUTION IN BRAZIL: AN UNCOMFORTABLE REALITY

EMERSON WENDT[1]

FILIPE DE MORAIS[2]

[1] Doutor (2023) e Mestre (2016) em Direito pela Universidade La Salle – Canoas/RS. Professor do Programa de Pós-Graduação em Direito da Universidade La Salle – Canoas/RS e líder do Grupo de Pesquisa Teorias Sociais do Direito. Editor-revisor da revista Direito & TI (www.direitoeti.com.br), Qualis B1 Capes. Delegado de Polícia Civil do Estado do RS. E-mail: emersonwendt@gmail.com. Lattes: http://lattes.cnpq.br/9475388941521093. Orcid: https://orcid.org/0000-0002-0195-5445.

[2] Delegado de Polícia no Estado de São Paulo. Mestre e doutor em Direito. Pós-graduado em Inteligência de Segurança Pública. Possui cursos de especialização na Academia de Polícia do Estado de São Paulo em Interceptações Telefônicas e Telemáticas, Investigação de Crimes Digitais e Coletas em Fontes Abertas, Investigação de Crimes de Lavagem de Dinheiro. Certificado em gestão de riscos – ISO 31000, Segurança da Informação – ISO 27000, LGDP, GDPR e *Cybersecutiry*. Foi titular do Setor de Homicídios e Proteção à Pessoa – Delegacia de Polícia Seccional de Santo André, assistente da Delegacia de Investigações Sobre entorpecentes – Delegacia de Polícia Seccional de Santo André. Assistente do 1.º Distrito Policial de São Bernardo do Campo e supervisor do Grupo de Operações Especiais – Delegacia de Polícia Seccional de São Bernardo do Campo. Titular da 4.ª Delegacia de Proteção à Pessoa – Repressão à Pedofilia/DHPP. Supervisor da Equipe B-Leste de investigações – 2.ª Delegacia de Repressão a Homicídios/DHPP. Supervisor da Equipe "A" de investigações – 1.ª Delegacia Antissequestro/DAS/DOPE. Lattes: https://lattes.cnpq.br/1729555016433618.

Consequências na Segurança Pública. Considerações finais: em busca de uma solução viável. Referências Finais.

RESUMO: O crescimento dos crimes digitais no Brasil, apesar da criação de tipos penais específicos, evidencia a insuficiência do atual modelo de política pública de persecução penal e da produção de provas digitais. Este artigo tem como objetivo analisar o impacto das medidas legislativas e estatais sobre a criminalidade digital e sua interação com o sistema de Segurança Pública brasileiro. A pesquisa adota abordagem qualitativa exploratória e descritiva, com suporte quantitativo a partir de dados oficiais e de organizações não governamentais, além de revisão bibliográfica, documental e estudos de caso oriundos de investigações reais nos estados de São Paulo e Rio Grande do Sul. Os resultados indicam que a fragmentação normativa, a insegurança jurídica na obtenção e manejo das provas digitais, e a ausência de um arcabouço processual penal adequado comprometem a eficácia da repressão criminal digital. Constatou-se ainda que a política de Segurança Pública, centrada no policiamento ostensivo preventivo, não está estruturada para demandas investigativas complexas inerentes à criminalidade digital, favorecendo a impunidade, a descapitalização insuficiente do crime e o fortalecimento de organizações criminosas difusas. Propõe-se, portanto, a criação de legislação específica que regule uniformemente a produção de provas digitais, distinguindo dados em repouso, em trânsito e em uso, e que contemple mecanismos emergenciais para requisição de dados, alinhada a padrões internacionais, como a Convenção de Budapeste e o Electronic Communications Privacy Act[3]. A contribuição principal reside na indicação de diretrizes legislativas e políticas criminais que promovam maior segurança jurídica e eficiência na persecução penal digital, fundamental para o enfrentamento da criminalidade contemporânea.

PALAVRAS-CHAVE: Crimes digitais. Provas digitais. Persecução penal. Segurança pública. Política criminal.

ABSTRACT: The growth of digital crimes in Brazil, despite the creation of specific criminal classifications, highlights the insufficiency of the current public policy model for criminal prosecution and the production of digital evidence. This article aims to analyze the impact of legislative and state measures on digital criminality and its interaction with the Brazilian Public Security system. The research adopts a qualitative, exploratory, and descriptive approach, with quantitative support from official data and non-governmental organizations, in addition to a literature review, documentary analysis, and case studies from real investigations in the states of São Paulo and Rio Grande do Sul. The results indicate that normative fragmentation, legal uncertainty in obtaining and handling digital evidence, and the absence of an adequate criminal procedural framework compromise the effectiveness of digital criminal repression. It

[3] UNITED STATES. **Electronic Communications Privacy Act of 1986 (ECPA)**. Public Law 99-508, 21 Oct. 1986. 100 Stat. 1848–1873. Washington, DC: U.S. Government Publishing Office, 1986. Disponível em: https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1848. Acesso em: 21/09/2025.

was also found that the Public Security policy, centered on preventive ostensive policing, is not structured for the complex investigative demands inherent to digital criminality, thus fostering impunity, insufficient decapitalization of crime, and the strengthening of diffuse criminal organizations. Therefore, the creation of specific legislation is proposed to uniformly regulate the production of digital evidence - distinguishing between data at rest, in transit, and in use - and to include emergency mechanisms for data requisition, aligned with international standards such as the Budapest Convention and the Electronic Communications Privacy Act. The main contribution lies in providing legislative and criminal policy guidelines that promote greater legal certainty and efficiency in digital criminal prosecution, which is fundamental for confronting contemporary criminality.

KEYWORDS: Digital crimes. Digital evidence. Criminal prosecution. Public security. Criminal policy.

INTRODUÇÃO: OS "CRIMES DIGITAIS" SÃO UM PROBLEMA DESCONHECIDO?

De acordo com o Anuário do Fórum Brasileiro de Segurança Pública[4], em 2024, ocorreram 281.206 estelionatos por meio eletrônico no Brasil. Ocorre que, dados oficiais mostram os estados da federação possuem abordagens distintas para quantificar os crimes ocorridos em suas circunscrições territoriais. O Estado de São Paulo – mais populoso do país – por exemplo, registrou naquele período 801.759 estelionatos, o que representa 71.1% acima da média nacional. Nesse sentido, não há dados sobre estelionatos ocorridos no meio digital. São todos estelionatos, para todos os fins.

O legislador tem criado outros crimes praticados na/pela *Internet*, formas qualificadas ou causas especiais de aumento de pena quando as condutas estão relacionadas ao ambiente digital. Essa circunstância está de acordo com a própria finalidade do Direito Penal que é a proteção de bens jurídico-penais essenciais[5].

Além da já mencionada Lei n.º 12.737/2012, a Lei n.º 13.968/19 incluiu os §§ 4.º e 5.º ao crime do Art. 122 do Código Penal (CP) – Induzimento, instigação ou

[4] FÓRUM Brasileiro de Segurança Pública. **19º Anuário Brasileiro de Segurança Pública.** São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: <https://publicacoes.forumseguranca.org.br/handle/123456789/279>. Acesso em: 21/09/2025. p. 105.

[5] Segundo Claus Roxin (2009, p. 61): "O Direito penal protege, no marco do alcance de seus tipos penais, os bens jurídicos frente aos riscos não permitidos." *In* ROXIN, Claus. **A proteção de bens jurídicos como função do direito penal**. 2.ª ed. Organização e tradução de André Luís Callegari e Nereu José Giacomolli. Porto Alegre: Livraria do Advogado, 2009.

auxílio a suicídio ou a automutilação – na medida em que reconheceu causas especiais de aumento de pena, quando aquele crime ocorre em ambiente digital. A Lei n.º 13.964/2019 incluiu o § 2.º ao Art. 141 tratando-se da aplicação da pena em dobro nos crimes contra a honra, quando cometidos na *Internet.* O *Cyberbullying*, criado pela Lei n.º 14.811/2024 – Art. 146-A, parágrafo único. A violência psicológica contra a mulher, na forma agravada, incluída pela Lei n.º 15.123/2025 – Art. 147-B, parágrafo único. A Lei n.º 14.155/2021 que criou as formas digitais dos crimes de furto qualificado – Art. 155, § 4.º-B e estelionato – Art. 171, § 2.º - A. A Lei n.º 13.718/2018 que criou o crime de *"Divulgação de cena de estupro ou cena de estupro de vulnerável, de cena de sexo ou de pornografia"* – Art. 281-C.

A Lei n.º 12.737/2012 também alterou o Art. 266, ao incluir como objeto material de crime, o fornecimento de acesso à *Internet*, além de outras modalidades de comunicação, notadamente a telegráfica ou telefônica. Igualmente, equiparou o cartão bancário a documento particular, para fins de crime de Falsificação de documento particular – Art. 298. Essas leis encerram os crimes digitais previstos no CP.

Além disso, a legislação penal especial também prevê condutas praticadas na *Internet*, por exemplo, o Estatuto da Criança e Adolescente – Lei n.º 8.069/1990, alterado pela Lei n.º 11.829/2008 que, entre outras condutas, incluiu o Art. 241-A:

> Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornografia envolvendo criança ou adolescente.

De fato, são muitas leis que criaram crimes com base na e para condutas praticadas pela *Internet*. Todos esses crimes, no entanto, possuem elevados indicadores, sem qualquer expectativa de redução significativa. Por exemplo, de acordo com o Anuário do Fórum Brasileiro de Segurança Pública[6] ocorreram, 6.319 e 7.175 casos do crime do Art. 218-C do CP nos anos de 2023 e 2024, bem como 2.543 registros de *Cyberbullying* em 2024[7].

Além dos crimes levados ao conhecimento do Estado, certamente há uma quantidade de crimes não comunicados, a chamada cifra oculta. Assim, pergunta-se qual o impacto das medidas estatais e legislativas, especialmente a criação de tipos

[6] Idem, p. 175.
[7] Ibidem, p. 228.

penais, sobre a criminalidade digital e sua interação com o modelo de [política pública de] Segurança Pública brasileiro?

A temática também levará em conta outras circunstâncias, que parecem passar despercebidas. Conquanto as pessoas tenham incorporado recursos da *Internet* em sua rotina diária, assim fizeram os criminosos na mesma proporção. Autores de homicídio podem se ajustar previamente para emboscar a vítima com uso de aplicativos de mensagens instantâneas. Traficantes de drogas podem compartilhar dados e comunicar-se com contas de *e-mail* e computação em nuvem. Sequestradores podem extorquir familiares da vítima em cativeiro com a função *SMS* e realizar sucessivas operações bancárias com aplicações de informática disponibilizadas por instituições financeiras. Portanto, pode-se afirmar todos os crimes tornaram-se 'digitais', em alguma medida, pois podem ser praticados com uso da Internet e a partir dela.

Dado esse contexto, a principal hipótese é a de que criação de tipos penais específicos para crimes digitais, embora necessária, não tem produzido impacto significativo na redução da criminalidade digital no Brasil devido à ausência de um arcabouço processual penal adequado para a produção de provas digitais, pautando-se por Wendt, em estudos complementares de 2017, 2023 e 2024[8].

Subsidiariamente, trabalhar-se-á com três hipóteses complementares: a primeira, de que o atual modelo de produção de provas digitais no Brasil é insuficiente e juridicamente inseguro, pois não distingue adequadamente entre dados em repouso, dados em trânsito e dados em uso, gerando conflitos entre normas processuais penais, legislação de proteção de dados e normas técnicas facultativas; a segunda, de que a política de Segurança Pública brasileiro, centrada no policiamento ostensivo preventivo e na tipificação penal reativa, não está estruturada para enfrentar a criminalidade digital, que demanda investimento em investigação criminal especializada e produção de provas técnicas complexas, e; a terceira, de que a insegurança jurídica na produção de provas digitais gera três consequências principais: (a) promoção da impunidade; (b) dificuldade na descapitalização do crime;

[8] *In*: WENDT, Emerson. **Internet & Direito Penal**: risco e cultura do medo. Porto Alegre: Livraria do Advogado, 2017; WENDT, Emerson. **As expectativas cognitivas e normativas dos atores de investigação policial em face dos crimes cibernéticos.** 2023. Tese (Doutorado em Direito) – Universidade LaSalle, Canoas, 2023; e, WENDT, Emerson. **Investigação criminal cibernética no Brasil**: legislação, estrutura e desafios. Leme: Editora Mizuno, 2024.

e (c) fortalecimento de organizações criminosas difusas que operam predominantemente em ambiente digital.

Para tanto, no decorrer dos tópicos, objetiva-se mapear a legislação brasileira sobre crimes digitais, analisar indicadores de criminalidade digital no Brasil, examinar a política criminal brasileira e sua relação com crimes digitais, avaliar os estudos acadêmicos sobre criminalidade e Segurança Pública, identificar problemas na produção de provas digitais, analisar casos concretos de investigações envolvendo provas digitais e, finalmente, propor diretrizes legislativas para enfrentamento do problema.

A abordagem metodológica para esse estudo é de natureza qualitativa com suporte quantitativo (dados estatísticos, especialmente a partir do Anuário do Fórum Brasileiro de Segurança Pública e do Instituto Sou da Paz), realizando-se a pesquisa de maneira exploratória e descritiva, com procedimentos de pesquisa e revisão bibliográfica, documental (legislação brasileira) e com estudos de caso (investigações reais).

Além de Wendt[9], a fundamentação teórica pauta-se em três eixos principais, quais sejam, o Direito Penal Material, a partir da análise de tipificação de crimes digitais, o Direito Processual Penal, a partir da produção de provas digitais, e, a Política Criminal e Segurança Pública, perpassando pela estrutura e política brasileira de enfrentamento e controle da criminalidade. Como não se trata de um estudo comparativo, deixa-se de trazer autores e referências estrangeiras.

Adverte-se de que esta pesquisa pode apresentar limitações temporais, pois os dados estatísticos referem-se ao período de 2023-2024, não indo muito além em razão de que o crescimento dos delitos na Internet ocorreram pós período da pandemia da Covid 19[10]; também, por limitações geográficas, pois os estudos de caso referem-se a investigações conduzidas nos estados de São Paulo e Rio Grande do Sul, podendo não refletir a realidade de outras unidades federativas; doutra parte, limitações metodológicas, porquanto a ausência de dados desagregados sobre crimes digitais em alguns estados (como São Paulo) limitou a análise comparativa; ainda, uma limitação de generalização, pois os estudos de caso, embora ilustrativos, não

[9] Idem.
[10] Veja-se os dados estatísticos de acordo com o Fórum Brasileiro de Segurança Pública, referenciados na sequência deste trabalho.

permitem generalização estatística para o universo de investigações criminais no Brasil.

2 CRIMES DIGITAIS E POLÍTICA CRIMINAL BRASILEIRA

A política criminal pode ser definida como o conjunto de medidas com o fim de promover o controle da criminalidade, no bojo dos poderes estatais – Executivo, Legislativo e Judiciário. Os estudos acadêmicos, notadamente criminológicos e jurídicos, mostram-se relevantes para o planejamento e execução da política criminal.

A Criminologia trata-se de ciência com método e técnicas únicos, ainda que a interdisciplinariedade seja uma de suas características essenciais. Ocorre que, a Criminologia tradicional passou a ser enxergada com desconfiança, por conta de vieses construídos no final do século XIX e ao longo do século XX.

Nesse sentido, a obra de Cesare Lombroso – 1835 -1909 – que, a partir de análises clínicas e estudos antropológicos, criou o chamado "criminoso nato". Conquanto ignorou outros elementos que colaborassem com a prática de crimes – sobretudo de natureza socioeconômica – sobre o trabalho de Lombroso recaem críticas – pertinentes – de uma Criminologia preconceituosa e voltada ao controle social de minorias.

Outras teorias criminológicas são dignas de referência, a exemplo da chamada das *"janelas quebradas"*, idealizada por James Quinn Wilson e George Lee Kelling – 1982 – que sustentaram pequenos vestígios de desordem no ambiente urbano, caso não fossem contidos com firmeza pelo Estado, necessariamente levariam a uma escalada da criminalidade. Ainda que considerasse elementos socioeconômicos – de natureza urbanística – a teoria das *"janelas quebradas"* também foi duramente criticada por estigmatizar e promover o controle social de minorais.

Por essas razões, os estudos criminológicos baseados em indicadores numéricos têm ganhado força no planejamento e execução da política criminal – inclusive no Brasil. De fato, a utilização de critérios dessa natureza é objetiva e livres de vieses, porquanto se fundamenta na realidade constatada e, a partir dela, o estabelecimento de políticas de enfrentamento.

Em relação ao Direito Penal, suas bases atuais foram construídas a partir das revoluções iluministas do final do século XIX, sobretudo a Independência dos Estados Unidos da América e a Revolução Francesa[11]. O momento histórico revelava os traumas sociais provocados pela aplicação sem limites de penas pelo regime das monarquias nacionais absolutistas. Portanto, o Direito Penal deveria ser aplicado com parcimônia e respeito a direitos e garantias individuais, devendo o Estado limitar seus próprios poderes. É desse período a criação do princípio da legalidade, da anterioridade penal, da intervenção mínima e do devido processo legal.

Com o surgimento do globalismo, a partir da metade do século XX, o Direito Penal reconheceu a existência de conflitos coletivos, contra bens jurídico-penais da mesma natureza, por exemplo, o meio ambiente, o consumidor, o sistema econômico e minorias sociais. No Brasil, destacam-se a Lei de Crimes Ambientais – Lei n.º 9.605/1998[12] – o Estatuto da Criança e Adolescente e o Código de Defesa do Consumidor – Lei n.º 8.069/1990 e Lei n.º 8.078/9190 que possuem suas próprias disposições penais. A Lei Maria da Penha – Lei n.º 11.340/2006 – que "cria mecanismos para coibir a violência doméstica e familiar contra a mulher".

As circunstâncias acima mencionadas resumem o perfil atual da política criminal brasileira:

- **Predomínio do policiamento ostensivo de natureza preventiva:** no Brasil, o policiamento uniformizado é realizado majoritariamente pelas polícias militares - § 5.º, do Art. 144 da Constituição Federal de 1988. Ainda que não estejam incluídas no rol daquele dispositivo, a interpretação sistemática da constituição em conjunto com a Lei n.º 13.022/2014 – Estatuto Geral das Guardas Municipais autoriza entender as Guardas Civis Municipais enquanto órgão de Segurança Pública de natureza preventiva[13]. A preferência pelo policiamento

[11] Leciona Luiz Luisi: "O Rechtssaats, produto das ideias iluministas dos séculos XVII e XVIII configura-se normativamente a partir da vigência das constituições americanas do segundo quartel no século XVIII e da constituição francesa de 1791. A sua tônica, é a afirmação dos direitos do homem e do cidadão e a limitação do papel do Estado a garantir a efetivação e eficácia dos mencionados direitos, principalmente no que concerne a inviolabilidade da liberdade individual e da propriedade." *In* LUISI, Luiz. **Princípios constitucionais penais**. 2.ª ed. rev. e ampl. Porto Alegre: Sérgio Antonio Fabris Editor, 2003. p. 11.

[12] Que aliás inaugurou no Brasil a ideia de crime praticado por pessoa jurídica.

[13] As discussões jurídicas sobre o assunto – aparentemente intermináveis – não impedem a realidade dos fatos: muitos municípios brasileiros possuem Guardas com efetivo superior ao da Polícia Militar, em suas circunscrições territoriais. Outrossim, muitas ocorrências de natureza criminal são apresentadas em distritos policiais por guardas civis municipais, diuturnamente, muito além das atribuições de defesa patrimonial do município.

ostensivo, inclusive, possui respaldo na doutrina do Direito, a pretexto de impedir as possíveis falhas na aplicação da lei penal[14].

- **Rígido controle do emprego da força:** diante da crescente insegurança jurídica em torno da atividade policial, notadamente em relação ao uso da força, o Estado tem se dedicado na criação de mais mecanismos de controle da atividade policial. Por exemplo, a Lei n.º 13.060/2014 que *"disciplina o uso de instrumentos de menor potencial ofensivo pelos agentes de segurança pública, em todo território nacional".* Recentemente, a Portaria n.º 855/2025 do Ministério da Justiça e Segurança Pública estabeleceu as diretrizes sobre o uso da fora pelos profissionais de segurança pública.
- **Tutela penal para a solução de conflitos sociais sensíveis:** como mencionado anteriormente, o Direito Penal tem se expandido para questões de natureza coletiva, envolvendo bens jurídico-penais coletivos e grupos sociais vulneráveis. A inovação no Direito Penal ocorre após o fato, em razão da notoriedade e comoção provocada por aquele, ainda que de forma isolada[15].
- **Despenalização de condutas:** paradoxalmente à expansão do Direito Penal, o reconhecimento de institutos despenalizadores. Merecem destaque a transação penal, a suspensão condicional do processo e a composição civil de danos – Art. 76, 89 e 74 da Lei n.º 9.099/1995. O acordo de não persecução penal – Art. 28 da Lei n.º 13.964/2019 – Pacote Anticrime. Também podem ser entendidas como despenalizadoras, as regras de progressão de regime prisional do Art. 112 a 118 da Lei n.º 7.210/1984, alteradas pelo Pacote Anticrime. A substituição de penas restritivas de liberdade por restritivas de direitos – Art. 44 e 43 do CP.

---

[14] Claus Roxin cita o exemplo da cidade de Munique, sendo essa a cidade mais segura da Alemanha, em razão do "mais intenso de todos os policiamentos, obtendo disso maior eficácia preventiva." *In* ROXIN, Claus. **Estudos de Direito Penal**. 2.ª ed. rev. Tradução de Luís Greco. Rio de Janeiro: Renovar, 2008. p. 08.

[15] A crítica de Sérgio Salomão Shecaira é pertinente: "Se o fato não se reitera, desnecessário tê-lo como delituoso. Um exemplo disso aconteceu, anos atrás, no litoral do Rio de Janeiro. Houve um encalhe de um filhote de baleia em uma praia carioca e um dos banhistas, que por ali passava, introduziu um palito de sorvete no orifício de respiração do animal. Pouco tempo depois, por pressão de entidades ambientalistas, o Congresso Nacional aprovou a lei de cinco artigos (Lei n.º 7.643/87) em que descrevia a suposta conduta praticada por aquele banhista: molestamento intencional de cetáceo (Art. 1.º com a atribuição de uma pena de 2 a 5 anos). Nem se pretende fazer crítica do verbo utilizado para descrever a conduta praticada por aquele agente, mas tão somente destacar a impropriedade de, por ocorrência única no país, promover aquele fato à condição de crime.". *In* SHECAIRA, Sérgio Salomão. **Criminologia**. 6.ª ed. rev. e atual. São Paulo: Revista dos Tribunais, 2014. p. 47.

- **Expansão de nulidades processuais:** o direito processual penal brasileiro possui muitos recursos pela defesa. Além disso, as nulidades processuais têm avançado, sobretudo por força de decisões tomadas pelas cortes superiores, muito além da expressão *pas de nullité sans grief*. Essa circunstância possui especial relevância com a criminalidade digital, como será abordado adiante.

3 PERSPECTIVAS ACADÊMICAS SOBRE O PROBLEMA

Como mencionado anteriormente, os estudos acadêmicos, sobretudo criminológicos e jurídicos, são um relevante instrumento para a formulação e execução da política criminal brasileira. Em relação aos estudos criminológicos, incorporaram elementos da estatística, na medida em que se baseiam em indicadores numéricos, de modo a proporcionar maior objetividade e clareza no diagnóstico do problema.

A metodologia atual de coleta de dados se dá por natureza criminal e produzida por órgãos oficiais ou organizações não governamentais vinculadas à Segurança Pública. Essa metodologia está de acordo com o perfil atual da política criminal brasileira, de natureza preventiva, com ênfase no policiamento ostensivo e na tipificação de condutas pelo legislador, entre outras medidas igualmente baseadas na prevenção imediata.

Ocorre que essa metodologia pouco ou nada diz a respeito da prevenção mediata produzida pela investigação criminal, no Brasil, uma função majoritariamente atribuída às Polícias Civis estaduais e Polícia Federal. A prevenção mediata produzida pela investigação criminal está associada a uma política criminal a médio e longo prazo que demanda ação planejada, porém com efeitos duradouros.

Nesse caso, os estudos existentes consideram indicadores de esclarecimento de crimes de forma isolada. Por exemplo, a 7.ª edição da pesquisa intitulada “Onde Mora a Impunidade?” do Instituto Sou da Paz informa que, no ano de 2022, o índice de esclarecimentos de homicídios pela Polícia é de 39%, sendo o critério adotado é o oferecimento de denúncia pelo Ministério Público. A justificativa (Instituto, 2024, p. 08) é a conjugação de entendimento entre dois órgãos distintos sobre o fato, a Polícia e o Ministério Público.

Esse critério é discutível por duas razões. O § 6.º do Art. 2.º da Lei n.º 12.830/2013 diz que o indiciamento, enquanto ato privativo do delegado de polícia, consiste na atribuição de autoria e materialidade do crime, fundamentadamente, durante a fase policial. Por fim, o indiciamento e oferecimento de denúncia podem resultar na absolvição do acusado, pelo Poder Judiciário, após o devido processo legal, por insuficiência de provas – inciso VII, Art. 386, do Código de Processo Penal (CPP).

Em realidade, organismos não governamentais de Segurança Pública pouco falam sobre as causas que colaboram com o esclarecimento de crimes no Brasil. Há estudos que alertam – corretamente – sobre a necessidade de maiores investimentos no policiamento investigativo, mas as recomendações são demasiadamente genéricas e já conhecidas por gestores de Segurança Pública[16] [17].

No caso do Direito, a produção acadêmica é voltada majoritariamente à discussão de elementos éticos, estéticos ou filosóficos daquele. Poucos estudos são voltados à solução concreta de problemas – inclusive a eficácia e eficiência de normas jurídicas – por meio da aplicação do método científico tradicional, o que estimula cada vez mais o distanciamento da execução da política criminal do exercício da jurisdição criminal.

4 MODELO/POLÍTICA DE POLICIAMENTO: E A INTERNET?

De fato, a política criminal brasileira contemporânea tornou-se uma balança muito difícil de manter-se equilibrada, considerando a pluralidade de vieses que

[16] Nesse sentido o Anuário do Fórum Brasileiro de Segurança Pública: “E, por conseguinte, investimentos em polícia judiciária e perícias técnicas, que poderiam aumentar a eficiência da investigação e reduzir a impunidade são lateralizados e pouco priorizados.” *In:* FÓRUM Brasileiro de Segurança Pública. **19º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: <https://publicacoes.forumseguranca.org.br/handle/123456789/279>. Acesso em: 21/09/2025. p. 107.

[17] Na publicação “Onde Mora a Impunidade” são elencadas medidas para incrementar os indicadores de esclarecimento de homicídios: (i) a capacitação de policiais na preservação de local de homicídio, (ii) a criação de equipes de polícia dedicadas à investigação daquele crime, (iii) a integração com o Ministério Público e (iv) o investimento em equipamentos de perícia. *In* INSTITUTO Sou da Paz. **Onde mora a impunidade?** Porque o Brasil precisa de um indicador nacional de esclarecimento de homicídios. 7. ed. São Paulo: Instituto Sou da Paz, 2024.

pretende contemplar, em comparação com os recursos disponíveis para efetivar aquela.

A incorporação de recursos da *Internet* pelo crime adicionou um novo elemento ao grave problema da criminalidade, cuja dimensão permanece desconhecida. Isso porque não se restringe àquilo que se convencionou chamar “crimes digitais”, mas sim, todos os crimes incorporaram algum recurso da *Internet*, em alguma medida. Alguns crimes, ainda que não sejam rotulados como ‘digitais’ possuem pertinência significativa com a matéria, inclusive no contexto de organizações criminosas. É o caso, por exemplo, do tráfico de drogas, da extorsão mediante sequestro e lavagem de dinheiro.

Todavia, como mencionado anteriormente, a política criminal brasileira é majoritariamente preventiva e isso se revela na adoção de modelo de policiamento. O policiamento ostensivo é amplamente adotado, por meio das Polícias Militares e Guardas Civis Municipais e sua relevância permanece na prevenção de crimes e manutenção da ordem pública. Entretanto, com a incorporação de recursos da *Internet* pelos criminosos, não há como negar uma massa de crimes são executados ou consumados além do alcance visual do policial uniformizado.

Isso inclui a utilização de sistema de monitoramento remoto por câmeras – estáticas ou móveis – ainda que a incorporação de tecnologias como o reconhecimento biométrico sejam oportunas, sobretudo no Brasil, onde há 373.991 mandados de prisão pendentes de cumprimento[18]. Porém, reforça-se o questionamento do título deste tópico: e a prevenção, sob a perspectiva da segurança pública, no âmbito da Internet? Precisamos de *cibercops*? Se sim, quais os limites de sua atuação, de monitoramento, acompanhamento, interação e *reports*.

5 PRODUÇÃO LEGISLATIVA

[18] BRASIL. Conselho Nacional de Justiça. **Cidadania nos presídios**. Brasília, DF: CNJ, [s.d.]. Disponível em:<https://www.cnj.jus.br/sistema-carcerario/cidadania-nos-presidios/>. Acesso em: 21/09/2025.

Como dito, o legislador brasileiro inova no sistema de leis penais por demanda[19]. Essa circunstância possui o inconveniente de retardar a implementação de política criminal planejada a médio e longo prazo, vide o exemplo do PLS n.º 236/2012 e o PLS 156/2009, respectivamente os projetos legislativos do novo Código Penal e Código de Processo Penal.

No caso de recursos da *Internet* incorporados pelo crime, o problema agrava-se. Como aludido, a primeira lei sobre crimes praticados em ambiente virtual foi a Lei n.º 12.737/2012, conhecida popularmente como "Lei Carolina Dieckmann", em alusão à famosa atriz da televisão brasileira. Em resumo, a vítima entregou dispositivo de telemática de sua propriedade para manutenção, quando sofreu extorsão, consistente na obtenção de vantagem patrimonial ilícita, de modo não fossem compartilhados dados e informações pessoais.

Ocorre que, conforme Wendt[20], o legislador criou um tipo penal consistente violar dispositivo de informática com o fim de obter, alterar ou destruir dados sem a concordância do titular. O mesmo tipo penal criminaliza a conduta de instalar ou disseminar programa malicioso, com o fim de obter finalidade ilícita, sendo a pena de 3 (três) meses a 1 (um) ano de detenção. A apuração ocorre de acordo com a manifestação da vontade da vítima, em regra.

A Lei n.º 12.737/2012 também alterou o Art. 266 do Código Penal, ao incluir como objeto material de crime, o fornecimento de acesso à *Internet*, além de outras modalidades de comunicação, notadamente a telegráfica ou telefônica. Finalmente, equiparou o cartão bancário a documento particular, para fins de crime de Falsificação de documento particular – Art. 298 do CP.

Há quem repute relevante o ingresso dessa norma, denominada de "Lei Carolina Dieckmann", no sistema de leis penais brasileiro, porém seus resultados concretos são insignificantes, tanto que os dados relacionados a esses crimes sequer são coletados, tanto por órgãos oficiais quanto por organizações não governamentais de estudos sobre Segurança Pública.

A conduta contra a atriz da televisão brasileira, ora vítima, enquadrou-se no crime de extorsão – Art. 158 do CP – pois, agrediu os bens jurídicos patrimônio e liberdade individual. Nesse caso, a pena é de reclusão de 4 (quatro) a 10 (dez) anos

---

[19] Ver Wendt, nas pesquisas de 2017 e 2023, referenciadas anteriormente.
[20] WENDT, Emerson. **Internet & Direito Penal**: risco e cultura do medo. Porto Alegre: Livraria do Advogado, 2017.

de reclusão. Além disso, a possibilidade de decretação da prisão temporária – alínea "d", inciso III, do Art. 1.º da Lei n.º 7.960/1989 para garantir a eficácia da investigação, notadamente a preservação do ânimo da vítima em participar dos atos da persecução penal.

Conclui-se, o Art. 154 – A do CP reserva-se a modalidades de ataques virtuais sem desdobramentos mais graves, nada que cuidados rotineiros de segurança não sejam suficientes. Não se aplica, sequer, à prática de *ransomware*, quando o autor exige o pagamento de resgate – daí a utilização da expressão em inglês *ransom* – ao usuário para acessar dados armazenados em dispositivo de telemática.

A inclusão da expressões "informático" ou "telemático" ao crime do Art. 266 do CP poderia ser reconhecida pela interpretação extensiva da norma. Não há que se falar em analogia *in malan partem*, pois não há criação de norma por aquele método.

A inclusão da expressão "cartão de crédito ou de débito" no Art. 298 do CP também poderia ser superada por interpretação extensiva da norma. No mais, em razão do princípio da consunção, a utilização de documento contrafeito é absorvida pelo crime mais grave, sobretudo no estelionato ou no furto qualificado com emprego de fraude.

À época da criação da Lei Carolina Dieckmann, eram recorrentes os furtos qualificados no interior de agências bancárias na modalidade "troca de cartão", entretanto, diante de novas técnicas empregadas por criminosos no ambiente virtual, essa técnica tornou-se obsoleta.

Em relação às penas, o crime descrito no Art. 154-A do CP recebeu tratamento de crime de menor potencial ofensivo, a ser processado nos termos da Lei n.º 9.099/95, considerando a pena aplicada é de 3 (três) meses a 1 (um) ano de detenção. Além disso a apuração está condicionada à manifestação de vontade da vítima.

Ora, a pena no Direito Penal possui caráter preventivo – prevenção geral e especial – entretanto, qual prevenção pretende-se atingir com patamares de penas tão baixos? Some-se a isso, os já mencionados institutos despenalizadores, como os já mencionados institutos da transação penal, a suspensão condicional do processo, a composição civil de danos, o acordo de não persecução penal e a substituição de penas restritivas de liberdade por restritivas de direitos.

E o padrão se repete em outras leis relacionadas a crimes praticados em ambiente digital. O crime de *Cyberbullying* – Art. 146-A, parágrafo único possui pena de reclusão, de 2 (dois) a 4 (quatro) anos, sendo que o juiz possui ampla

discricionariedade para aplicar o regime inicial aberto ou mesmo aplicar algum instituto despenalizador.

A causa de aumento de pena prevista no parágrafo único do Art. 147-B – violência psicológica contra a mulher, autoriza aplicação em dobro da pena quando utilizado recurso da *Internet*, sendo que a pena prevista no *caput* é de reclusão de 6 (seis) meses a 2 (dois) anos, e multa.

Os crimes de furto digital – Art. 155, § 4.º-B e fraude digital Art. 171, § 2.º-A, de fato, possuem patamares de penas mais elevados e condizentes com a realidade, de fato. Porém, por se tratar de crimes sem violência ou grave ameaça, mais uma vez, o juiz tem ampla discricionaridade para aplicar o regime aberto ou institutos despenalizadores, ainda que o prejuízo patrimonial da vítima seja elevado.

Por fim, o crime do Art. 218-C que descreve grave conduta contra a infância e juventude, apenado com reclusão de 1 (um) a 5 (cinco) anos. Demais disso, a Lei Carolina Dieckmann – assim como todas as outras que descrevem crimes digitais - nada diz a respeito da coleta de evidências daquela natureza, para fins de persecução penal.

6 PRODUÇÃO DE PROVA DIGITAIS – DADOS EM POSSE DO CONTROLADOR

São duas modalidades de dados digitais de interesse para a investigação criminal, em poder do controlador ou armazenados em dispositivo de telemática. Nesse caso será discutido o problema em torno dos dados em poder do controlador[21].

Existem três regimes jurídicos de produção de provas digitais no Direito brasileiro, naquela modalidade.

- **Com aplicação da cláusula de reserva de jurisdição:** nesse caso, a produção de provas de natureza digital ocorre com a concordância do Poder Judiciário. É o caso da Lei n.º 9.296/1996 – Lei de Interceptações Telefônicas, assim como o Art. 10 e seguintes da Lei n.º 12.965/2014 – Marco Civil da *Internet*. Tendo em vista a disseminação de instituições financeiras e

[21] O inciso VI do Art. 5.º da Lei n.º 13.709/18 - Lei Geral de Proteção de Dados, define controlador como: *"pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais."*.

operações bancárias digitais, a Lei Complementar n.º 105/2001 que regula o sigilo bancário, também se enquadra nessa modalidade.

- **Requisição pelo delegado de polícia ou membro do Ministério Público:** a produção da prova digital ocorre diretamente, sem a intervenção do Poder Judiciário. Por exemplo, o § 2.º, do Art. 2.º da Lei n.º 12.830/2013, assim como Art. 15 da Lei n.º 12.850/2013 e Art. 17-B da Lei n.º 9.613/1998, respectivamente, Lei de Organizações Criminosas e Lei de Lavagem de Dinheiro. O § 3.º, do Art. 10 da Lei n.º 12.695/2014 e o Art. 13-A do CPP.
- **Por convalidação posterior do Poder Judiciário:** o § 4.º do Art. 13-B do CPP informa que, nos crimes relacionados no artigo anterior, quando não houver manifestação judicial em até 12 (doze) horas, o delegado de polícia poderá requisitar ao controlador dados de localização da vítima e investigados pelo crime, devendo o inquérito policial ser instaurado em até 72 (setenta e duas) horas após o fato[22].

Como observado anteriormente, todas as modalidades de crimes incorporaram, em alguma proporção, recursos próprios da *Internet*. Portanto, o problema sobre a produção de prova digitais, no sistema de leis penais e processuais penais é decisiva para o enfrentamento do problema da Segurança Pública, muito além dos 'crimes digitais'. Foram identificados os seguintes problemas:

- **Ausência de uniformidade:** a legislação brasileira sobre a produção de provas digitais é esparsa e confusa, sendo que a inovação pelo legislador ocorre por demanda. Tal como na produção de leis materiais, essa circunstância impede a formulação e implementação de política criminal a médio e longo prazo e retarda a discussão de medidas mais oportunas que outras. Como mencionado anteriormente, a produção de provas digitais quando os dados se encontram em poder do controlador sujeita-se a três regimes jurídicos distintos, ao longo do CPP, leis penais especiais. Há também a incidência de normas genéricas de utilização da internet para fins civis, como o Marco Civil da *Internet* que disciplinou o acesso a *logs* de acesso a aplicação, registros de conexão por IP e outros dados relevantes para a investigação.

[22] Veja-se sobre o enfrentamento crítico do tema, a partir da perspectiva dos policiais, em WENDT, Emerson. **Investigação criminal cibernética no Brasil**: legislação, estrutura e desafios. Leme: Editora Mizuno, 2024.

- **Lacunas na lei ou emprego de expressões inadequadas:** talvez o exemplo mais evidente do emprego de expressões inadequadas ou redação confusa pelo legislador seja o inciso XII do Art. 5.º da CF de 88 que estabelece todas as formas de comunicação são invioláveis, exceto a telefônica, nos termos da lei. Ainda que a Lei de Interceptações Telefônicas tenha disciplinado o instituto e, mais recentemente a interceptação telemática e a captação ambiental, nada diz a respeito de dados pretéritos associados, por exemplo, bilhetagem, apontamento de ERB, *logs* de aplicação ou registros de conexão por IP.

Outro exemplo, que merece uma análise mais detida, diz respeito ao poder de requisitar dados cadastrais pelo delegado de polícia ou membro do Ministério Público, isto é, sem a intervenção do Poder Judiciário. Como mencionado anteriormente, a requisição de dados cadastrais está prevista de forma esparsa em leis penais especiais e no Código de Processo Penal.

Não se trata, porém, de um instituto novo no Direito brasileiro.

A Lei Complementar n.º 70/1991 instituiu uma nova modalidade de tributo, a Contribuição para o Financiamento da Seguridade Social – COFINS, assim como elevou as alíquotas de contribuição social sobre o lucro de instituições financeiras. O Art. 12 estabeleceu a prerrogativa da autoridade tributária, no exercício do Poder de Polícia Administrativa, requisitar dados cadastrais de contribuinte às instituições financeiras, com a finalidade de fiscalizar o pagamento daquele tributo, nos seguintes termos:

> [...] informações cadastrais sobre os usuários dos respectivos serviços, relativas ao nome, à filiação, ao endereço e ao número de inscrição do cliente no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Geral de Contribuintes (CGC).[23]

Daí surgiu a doutrina de Tércio Sampaio Ferraz Júnior[24] donde a inviolabilidade do sigilo prevista no XII do Art. 5.º da CF de 88 restringe-se à transmissão de dados em tempo real e não aos dados em si considerados. Ou seja, os dados que fossem

---

[23] BRASIL. **Lei Complementar nº 70, de 30 de dezembro de 1991**. Institui contribuição para financiamento da Seguridade Social, eleva a alíquota da contribuição social sobre o lucro das instituições financeiras e dá outras providências. Diário Oficial da União, Brasília, DF, 31 dez. 1991, Seção 1, p. 31057.

[24] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, Universidade de São Paulo n.º 88, p. 439-459, 1993. p. 447.

transmitidos e permanecessem armazenados – nesse caso pelo controlador – não seriam objeto de sigilo.

Em relação aos dados cadastrais, assim entendidos como dados pessoais coletados pelo controlador para o exercício de sua atividade, Tércio Sampaio Ferraz Júnior afirma – com razão – não se sujeitam se sujeitam à cláusula de sigilo: *"*Em consequência, simples cadastros de elementos identificadores (nome, endereço, RG, filiação, etc.) não são protegidos."[25]. Isso porque esses dados nada revelam sobre a privacidade e intimidade de pessoas e 'são informadas sem constrangimento'.

A tese de Tércio Sampaio Ferraz Júnior foi acolhida pelo Supremo Tribunal Federal, isto é, a proteção ao sigilo restringe-se à transmissão de dados e não aos dados em si, porém assim o fez casuisticamente[26]. Por essa razão, na jurisprudência das cortes superiores já foi decidido o delegado de polícia requisitar registros de ligações e acionamento de ERB pretéritos sem a intervenção do Poder Judiciário – HC 91.867, Relator Ministro Gilmar Mendes, 19/09/2012 – e, também pelo STJ – HC 66.368, Relator Ministro Gilson Dipp, DP 29/06/2007 – HC 247.331, Relatora Ministra Maria Thereza de Assis Moura, DJe 03/09/2014.

De fato, a doutrina de Tércio Sampaio Ferraz Júnior precisa ser revista, mas tão somente por conta dos avanços da tecnologia, desde que aquela foi construída. Àquela época, a telefonia móvel dava seus primeiros passos. Não havia aplicativos de comunicações instantâneas, muito menos armazenamento de dados em nuvem. Portanto, é razoável entender que a cláusula de sigilo se restringe aos dados cadastrais.

Ocorre que o legislador andou muito mal ao definir dados cadastrais. Em todos os casos, elencou somente dados convencionais, a exemplo, de nome, filiação,

---

[25] Idem, p. 449.

[26] Segundo Rafael Mafei Rabelo Queiroz e Paula Pedigoni Ponce, a incorporação da tese de Tércio pelo STF foi seletiva, na medida em que: "para além da distinção entre dados armazenados ou em trânsito comunicativo, Ferraz Júnior também afirmava que, embora a proteção constitucional do sigilo (inciso XII do Artigo 5.º) não alcançasse dados armazenados, o acesso a eles seria balizado pela guarida constitucional da privacidade (inciso X do mesmo artigo). Isto é, seria relevante avaliar em que medida o acesso aos dados armazenados no hard disk violaria a intimidade do indivíduo: mesmo que eles não pudessem ser chamados de 'sigilosos', nada impediria que fossem considerados, por exemplo, 'íntimos', e contassem com proteção condizente a esse status.". In QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, São Paulo, v. 1, n. 1, p. 64–90, fev. 2020. Disponível em: <https://revista.internetlab.org.br/tercio-sampaio-ferraz-junior-e-sigilo-de-dados-o-direito-a-privacidade-e-os-limites-a-funcao-fiscalizadora-do-estado-o-que-permanece-e-o-que-deve-ser-reconsiderado/>. Acesso em: 21/09/2025. p. 73.

estado civil e profissão, sendo que excluiu qualquer identificador digital do escopo da expressão ‘dados cadastrais’. Essa circunstância permitiu que, em realidade, os controladores ditassem a os limites de requisição de dados cadastrais pelo delegado de polícia ou membro do Ministério Público.

De modo a encerrar a celeuma foram propostos o Projeto de Lei n.º 1.515/2022[27], de autoria do deputado federal Coronel Armando, e o Projeto de Lei n.º 4.143/2023[28], do deputado federal Delegado Palumbo, definem corretamente dados cadastrais como:

> aqueles apresentados pelo titular para realização ou manutenção do cadastro perante particular ou Poder Público, abrangendo as informações referentes à qualificação pessoal, dados biométricos, filiação, endereço de assinante ou de usuário registrado ou autenticado para a conexão, identificação de usuário ou código de acesso que tenha sido atribuído no momento da conexão, além daqueles previstos no artigo 4.º inciso III e alíneas, da Lei n.º 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados.

Infelizmente, a discussão e aprovação dos referidos projetos de lei ficou para depois, por assim dizer.

Talvez a insegurança jurídica sobre o tema seja afastada, com a adesão do Brasil à Convenção sobre o Crime Cibernético – Convenção de Budapeste – por meio do Decreto n.º 11.491/2023. Nesse sentido, dados cadastrais são definidos pelo Art. 18, 3, nos seguintes termos:

> Para os fins do presente artigo, a expressão “dados relativos aos assinantes” designa qualquer informação, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida por um fornecedor de serviços e que diga respeito aos assinantes de seus serviços, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar: a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num

[27] BRASIL. Câmara dos Deputados. **Projeto de Lei n.º 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2326300>. Acesso em: 21/09/2025.

[28] BRASIL. Câmara dos Deputados. **Projeto de Lei n.º 4.143, de 2023**. Altera a Lei n.º 12.830, de 20 de junho de 2013, que dispõe sobre a investigação criminal conduzida pelo Delegado de Polícia. Brasília, DF: Câmara dos Deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2382762>. Acesso em: 21/09/2025.

> contrato ou acordo de serviços; c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

Ou seja, além dos dados pessoais convencionais, a exemplo de nome, filiação, telefone, endereço são considerados dados cadastrais contas de *e-mail*, assim como dados de conexão ou geolocalização à época da contratação do serviço e dados de localização ou identificação do respectivo dispositivo de comunicação.

Esses dados são coletados de acordo com a discricionariedade do controlador, para a execução do negócio, porém, não podem ser selecionados por aquele no momento de prestar esclarecimentos à autoridade requisitante. Por exemplo, o controlador de dados coleta os seguintes dados: a) Nome completo e data de nascimento; b) endereço físico; c) telefone e conta de *e-mail* e d) IP de conexão, data e hora no momento da contratação do serviço. São esses portanto, os dados cadastrais a serem informados, não podendo selecionar esse ou aquele meramente por conta da própria interpretação sobre o assunto.

- **Resistência indevida de controladores de dados:** a negativa indevida de controladores de dados é tratada como crime de desobediência – Art. 330 do CP, cuja pena é de 15 (quinze) dias a 6 (seis) meses, e multa. No contexto de investigação de organizações criminosas, o fato é tratado pelo Art. 21 da Lei n.º 12.850/13, cuja pena é reclusão de 6 (seis) meses a 2 (dois) anos, e multa. A falta de mecanismos mais eficientes, associada à falta de clareza das leis que regulam o tema estimulam a resistência indevida por controladores de dados, no descumprimento de prazos para prestarem esclarecimentos ou negativa indevida. A recusa revela-se também com a discussão em juízo sobre a validade de regras sobre a produção de provas de natureza digital, a exemplo da ADI 5059 e ADI 5642, ambas propostas pela Associação das Operadoras Celulares – ACEL.

Uma última questão merece uma análise mais detida. O Art. 50 da LGPD determina aos controladores de dados criarem suas próprias políticas de governança de dados, o que traz mais insegurança jurídica sobre o tema, inclusive com a adoção de normas técnicas internacionais, de natureza facultativa.

Um estudo de caso merece atenção sobre o tema. Uma investigação sobre homicídio foi iniciada pela Polícia Civil. Em resumo, o local tratava-se de um ponto de prostituição de travestis, sendo que pessoa que se servia de relações sexuais

mediante paga efetuou disparos de arma de fogo contra a vítima, assim como em direção à via pública, colocando em risco a vida e integridade física de terceiros.

Ao longo das investigações, apurou-se que a travesti mantinha uma conta bancária e uma máquina de pagamentos do cartão para o exercício de suas atividades. Por essa razão, o afastamento do sigilo bancário foi determinado pelo Poder Judiciário.

A instituição financeira prestou esclarecimentos. De fato, havia uma transferência no valor de R$ 50,00 (cinquenta reais) no extrato bancário da conta titularizada pela vítima, a indicar aquela foi realizada pelo autor do crime.

A instituição financeira nada esclareceu sobre a identificação do pagador, sequer o número do cartão bancário utilizado no pagamento, sendo essa informação imprescindível para o esclarecimento do caso. Para tanto, o corpo jurídico da instituição financeira alegou conformidade com a norma PCI-DSS[29], tratando-se de um padrão internacional de segurança adotado por operadoras de cartão bancário.

Ocorre que, assim como todas as outras normas técnicas, a PCI-DSS não recomenda o descumprimento de normas obrigatórias, nesse caso a Lei Complementar n.º 105/2001, que disciplina o sigilo bancário: *"If any of the requirements contained in this standard conflict with country, state, or local laws, the country, state, or local law will apply."*.

A Polícia Civil provocou novamente o Poder Judiciário com a apresentação dos termos da norma PCI-DSS, quando a instituição financeira informou o número do cartão bancário do autor do crime. Após, a expedição de mandado de busca e apreensão domiciliar, o autor foi preso em flagrante delito por posse ou porte ilegal de arma de fogo de uso restrito, pois foi encontrado um revólver calibre .38 SPL, assim como uma pistola calibre .380 AUTO, ambos com numeração suprimida e munições. A prisão preventiva foi decretada e, ao término do processo foi condenado à pena de 13 (treze) anos de prisão. Esse estudo de caso demonstra que a insegurança jurídica na produção de provas digitais precisa ser corrigida imediatamente, eis que muito além da questão dos crimes digitais em si. Mais uma vez, todos os crimes, não importa a natureza, em alguma proporção incorporaram recursos da rede mundial de computadores.

---

[29] PCI SECURITY STANDARDS COUNCIL. Payment Card Industry Data Security Standard (PCI DSS): **Requirements and Testing Procedures**. v. 4.0.1, jun. 2024. Disponível em: <https://www.pcisecuritystandards.org/document_library/> (PCI DSS v4.0.1). Acesso em: 21/09/2025.

- **Ausência de disciplina para dados emergenciais:** não há uma disciplina no Brasil sobre a requisição de dados em caráter emergencial, em casos excepcionais, a exemplo de extorsão mediante sequestro, desaparecimento, tráfico de pessoas, ataques em massa etc. O procedimento do Art. 13-B fala em requisição de dados após ausência de manifestação do Poder Judiciário em 12 (doze) horas. De fato, o procedimento do Art. 13-B está muito aquém das demandas produzidas em razão da comunicação de situações emergenciais. Ora, após 12 (doze) horas, a vítima de sequestro poderá ser morta pelos sequestradores, o agressor em massa poderá ter realizado seu ataque vitimando dezenas de pessoas. Atualmente, os dados são fornecidos por controladores nacionais na base do bom senso, enquanto controladores estrangeiros, principalmente estadunidenses, utilizam o *Electronic Comunications Privacy Act – Code § 2702, (b) Exceptions for Disclosure of Communications:*

> *A provider described in subsection (a) may divulgue the contentes os a communication – (8) to a governamental Entity, if the provider, in good faith, believes that na emergency involving Danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.*[30]

7 PRODUÇÃO DE PROVA DIGITAIS – DADOS ARMAZENADOS EM DISPOSITIVO

Atualmente, todos os dispositivos digitais incorporaram a função de conectar-se à Internet. Essa circunstância é relevante para fins de investigação criminal, na medida em que armazena dados de diversas naturezas, a exemplo de registros telefônicos convencionais, utilização de aplicações, acesso a sítios na *Internet* e documentos de todos os tipos.

A Lei n.º 13.964/2019 introduziu no Direito brasileiro o instituto da Cadeia de Custódia, tratando-se do processo que disciplina a produção de prova – de qualquer

[30] UNITED STATES. **Electronic Communications Privacy Act of 1986 (ECPA)**. Public Law 99-508, 21 Oct. 1986. 100 Stat. 1848–1873. Washington, DC: U.S. Government Publishing Office, 1986. Disponível em: <https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1848>. Acesso em: 21/09/2025.

natureza – desde a sua coleta, até o descarte. Apesar do avanço legislativo sobre o tema, o instituto tem suscitado discussões aparentemente intermináveis sobre a produção de provas, a partir de dados armazenados em dispositivo de telemática.

Por essa razão tem sido invocada ABNT NBR ISO 27037[31], como referência normativa na coleta e aquisição de dados em dispositivo de telemática, em processos judiciais de natureza criminal. Apesar de sua relevância, por se tratar de uma norma que estabelece padrões técnicos, o seu cumprimento é facultativo, ao contrário de leis produzidas pelo Poder Legislativo e atos administrativos normativos editados pela Administração Pública. A própria ABNT NBR ISO 27037 dispõe que: "A aplicação desta Norma requer conformidade com leis, regras e regulamentos nacionais. É recomendado que ela não substitua exigências legais de qualquer jurisdição."[32]

Essa disposição, por si só, já afasta a eventual alegação de nulidade na produção de provas digitais, em razão do descumprimento da ABNT NBR ISO 27037[33]. Demais nulidades decorrentes do processo de tratamento de evidências digitais devem ser suscitadas pela parte, sendo necessário a demonstração de prejuízo. Isto é, não basta alegar violação de Cadeia de Custódia, sem apontar qual etapa foi suprimida. O prejuízo é demonstrado a partir da realização de contraperícia, devendo o assistente pericial indicar que a evidência produzida não atende aos requisitos da auditabilidade, repetibilidade, reprodutibilidade, os quais asseguram a idoneidade e integridade do elemento de prova[34].

Não há, portanto, falar-se de nulidade por supressão de etapas descritas na ABNT NBR ISO 27037, isoladamente. Além da facultatividade da norma, ela descreve um cenário hipotético do encontro de um dispositivo digital, o qual é chamado de local de incidente. Em seguida, a norma descreve dezenas de atividades, ao longo das etapas descritas do processo de coleta de evidências digitais, que simplesmente podem não se aplicar ao caso concreto. Inclusive, as etapas da Cadeia de Custódia obrigatória – do CPP – não correspondem com as etapas da ABNT NBR ISO 27037.

---

[31] ASSOCIAÇÃO Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27037:2013** — Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2013.
[32] Idem.
[33] Idem.
[34] Nesse sentido, o HC 828.054 RN do Superior Tribunal de Justiça.

8 CONSEQUÊNCIAS NA SEGURANÇA PÚBLICA

Exaustivamente observado neste artigo, o reconhecimento em relação aos *crimes digitais*, isto é, aqueles que percorrem o *iter* do começo ao fim em meio digital, é oportuno e necessário, porém ainda insuficiente para fins de planejamento e execução da política criminal brasileira. Em alguma medida, todos os crimes incorporaram algum recurso da rede mundial de computadores, não havendo estudos sobre o verdadeiro impacto na Segurança Pública, relacionados a essa circunstância.

Em todo caso, o ponto central é a atual ausência ou insuficiência de regras adequadas sobre a produção de elementos de prova de natureza digital, a qual produz as seguintes consequências negativas:

- **Promoção da impunidade:** a ausência de regras adequadas para produção de provas digitais prejudica o esclarecimento de crimes e colabora com a impunidade. Essa circunstância é agravada considerando a criminalidade – mesmo a criminalidade ordinária – possui grande capacidade para reunir recursos materiais e humanos para a prática de crimes. Por exemplo, habilitar linhas telefônicas móveis, contas de *e-mail* ou contas bancárias com dados cadastrais fraudulentos ou dados pessoais de pessoas recrutadas para a prática de crimes, na condição de partícipes.
- **Descapitalização do crime:** a recuperação de ativos oriundos de crime também é medida para prevenir e reprimir crimes, assim como restaurar o sistema financeiro. Alessandro Gonçalves Barreto e Emerson Wendt afirmam que “a repressão correta ao crime de uma forma geral só pode ser feita se houver um ataque financeiro ao criminoso e/ou à organização”[35]. Diante da proliferação de instituições financeiras digitais e operações bancárias da mesma natureza, a existência de regras adequadas para a produção de provas digitais é medida que se impõe.
- **Fortalecimento do crime organizado:** a incorporação de recursos da *Internet* pelo crime, permitiu o surgimento de organizações criminosas difusas, sem a rígida estrutura hierárquica das organizações criminosas que permanecem no

[35] BARRETO, Alesandro Gonçalves; WENDT, Emerson. **Inteligência e investigação criminal em fontes abertas**. 4.ª ed. Rio de Janeiro: Brasport, 2024. p. 43.

modelo tradicional de atuação, com a prática de extorsões, loterias não autorizadas, tráfico de drogas, entre outros[36]. A divisão de tarefas é independente, com alta capacidade de recrutar recursos materiais e humanos. É o caso dos grupos de aplicativos de mensagens instantâneas, cujos participantes que cedem suas contas bancárias para o recebimento e ocultação de valores oriundos de crime, mediante paga. Esses "conteiros" na maioria das vezes não possuem antecedentes criminais e possuem ocupação lícita, sendo que são recrutados e gerenciados por um criminoso vinculado ou não diretamente ao núcleo da execução direta de crimes. Como não há disputa de território, essas organizações criminosas difusas convivem pacificamente e até atuam em colaboração com outras.

CONSIDERAÇÕES FINAIS: EM BUSCA DE UMA SOLUÇÃO VIÁVEL

A construção de uma solução para o impasse das regras sobre produção de provas digitais deve reconhecer os crimes, qualquer seja a natureza, incorporaram recursos da *Internet*. De nada adianta tipificar condutas praticadas na *Internet,* sem os recursos legais adequados para a sua investigação. Nesse sentido, três eixos principais são decisivos:

- Comunicação: a *Internet* permite maior velocidade, praticidade e adaptabilidade nas comunicações, por meio de serviços de *e-mail*, mensagens de texto, voz ou vídeo, que permanecem armazenadas com algum recurso da tecnologia. Chamadas de voz e vídeo, em tempo real, entre dois ou mais interlocutores, simultaneamente.

[36] Sobre a prática de extorsão e o surgimento do crime organizado, Marcelo Batlouni Mendroni diz que: "Também é atividade bem típica das organizações criminosas, que assim agem tendo pelo conhecimento do temor que conseguem impor às vítimas, ameaçando-as de ações violentas, como sequestro e assassinato, sendo, por isso mesmo, a melhor forma que as organizações criminosas têm para fixar o controle do território. A prática da extorsão é a mais comum e corriqueira das grandes organizações, estando presente em todas as máfias italianas, na máfia ítalo-americana, nas tríades chinesas, na máfia russa, etc. É, por assim dizer, o 'carro-chefe' dos crimes que praticam em razão do alto poder de intimidação que é capaz de impor às vítimas. Empresários e comerciantes colaboram mensalmente com uma quantia predeterminada pelos integrantes da organização, sob pena de sofrerem atentados de toda sorte: assassinatos, sequestros, ameaças de parentes e/ou amigos, explosões e incêndios contra as suas empresas e lojas etc.". *In* MENDRONI, Marcelo Batlouni**. Crime organizado**: aspectos gerais e mecanismos legais. 3.ª ed. São Paulo: Atlas, 2009. p. 192.

- Armazenamento e compartilhamento de dados: além de dispositivos convencionais de armazenamento digital, tecnologias de armazenamento e compartilhamento de dados virtuais – computação em nuvem – associadas a contas de *e-mail*. Aplicações de comunicação instantânea também incorporaram a funcionalidade de compartilhamento de documentos e arquivos de mídia.
- Comércio de bens e serviços *online*: utilização de plataformas virtuais de comércio de bens ou prestação de serviços por criminosos, tanto para praticar crimes, quanto como usuários finais.

Em seguida, é preciso compreender que dados digitais invariavelmente estão em poder do controlador ou armazenados em dispositivo digital.

No caso de dados em poder do controlador, com referência na classificação da Tecnologia da Informação, podem ser classificados como dados em repouso, dados em trânsito e dados em uso. Nesse sentido, dados cadastrais são dados em repouso, pois simplesmente foram informados pelo titular voluntariamente, à época da compra de bem ou contratação de serviço, sendo que o controlador simplesmente armazenou esses dados, não havendo que se falar em transmissão.

Dados em trânsito são aqueles que foram armazenados pelo controlador por qualquer meio, o que inclui bilhetagem, apontamento de ERB, *logs* de acesso, registros de conexão por IP, conteúdo de comunicações e compartilhamento de dados de qualquer natureza entre dois assinantes do mesmo serviço.

Finalmente, os dados em uso, são os dados em processamento, transmitidos em tempo real. Nesse caso e no caso dos dados em trânsito, por revelarem elementos da intimidade ou privacidade, sujeitam-se à reserva de sigilo. Em resumo:

Quadro: resumo sobre dados em repouso, trânsito ou em uso

Classificação	**Descrição**	**Sigilo**
Dados em repouso	Dados pessoais informados voluntariamente para compor cadastro de controlador de dados, por exemplo, nome, filiação, data de nascimento, estado civil, profissão, *e-mail*, identificadores de dispositivo de comunicação, geolocalização e dados de conexão no momento da contratação.	Não
Dados em trânsito	Dados armazenados por qualquer meio que revelam elementos da intimidade e/ou privacidade, por exemplo, *logs* de acesso, registros de conexão por IP, bilhetagem, apontamentos de ERB, conteúdo de	Sim

	comunicações e compartilhamento de dados entre interlocutores.	
Dados em uso	Transmissão em tempo real de comunicação ou dados de qualquer natureza.	Sim

Fonte: os autores (2025)

No caso de dados armazenados em dispositivo de telemática por armazenarem transmissão de dados de qualquer natureza e que revelam elementos da intimidade e privacidade, em todas as hipóteses impõe-se a cláusula de sigilo, podendo ser suprida com a expedição de mandado de busca e apreensão domiciliar, já que a alínea "f", do § 1.º, Art. 240, fala em "apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato;". Esse entendimento já foi consolidado no HC n.º 372.762 – MG do STJ.

No mais, as novas disposições antes propostas poderiam ingressar em uma nova lei de interceptações telefônicas, contemplando tanto a comunicação telefônica tradicional, quanto a transmissão de dados. Desta forma, dados em repouso a serem requisitados pelo delegado de polícia ou membro do Ministério Público, sendo que dados em trânsito e dados em uso sujeitos à cláusula de sigilo.

A única exceção aos dados em trânsito, notadamente de natureza geolocacional, apontamentos de ERB, *logs* de aplicação e registros de conexão por IP a serem requisitados ao respectivo controlador nos casos específicos de iminente e grave risco à vida e integridade física de pessoas. Trata-se, pois, da solução adotada pela ECPA[37].

Nos Estados Unidos da América, a lei que disciplina a interceptação do fluxo de comunicações telefônicas ou telemáticas é o *Eletronic Communications Privacy Act of 1986* que atualizou a lei anterior, conhecida como "Lei Federal de Escutas Telefônicas de 1968". No portal do *Bureau Of Justice Assistence,* o escopo do ECPA é o seguinte:

> *The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in*

[37] UNITED STATES. **Electronic Communications Privacy Act of 1986 (ECPA)**. Public Law 99-508, 21 Oct. 1986. 100 Stat. 1848–1873. Washington, DC: U.S. Government Publishing Office, 1986. Disponível em: <https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1848>. Acesso em: 21/09/2025.

> *transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically.*[38]

Importante: a lei também compreende dados armazenados em dispositivos digitais, podendo ser adotada a mesma solução para afastar qualquer divergência a respeito da Cadeia de Custódia do Código de Processo Penal.

De modo a respeitar eventuais distinções regionais, uma eventual lei relacionada ao sigilo telefônico e telemático poderia trazer diretrizes gerais sobre a coleta e aquisição de dados em dispositivos digitais autorizando os estados-membros da federação criar disposições de exclusivamente de natureza técnica, mediante ato administrativo normativo.

De outra parte, a partir das observações tratadas neste trabalho, pode-se ressaltar que a mera tipificação penal de condutas digitais é insuficiente sem um sistema processual penal robusto e adaptado às especificidades da prova digital, e, ao mesmo tempo, enfatizar que a insegurança jurídica na produção de provas digitais não apenas compromete a persecução penal, mas também fortalece o crime organizado e prejudica a segurança pública como um todo.

Ainda, projetando o futuro e melhorias inerentes à temática, sugere-se:

(a) a criação de um órgão ou força-tarefa especializada em crimes digitais, com recursos tecnológicos e humanos adequados, também focado em prevenção, com *cibercops* treinados para monitoramento e registro dos dados e evidências;

(b) a implementação de protocolos padronizados para coleta, preservação e análise de provas digitais, com base em normas técnicas e legais; e

(c) a revisão e atualização periódica da legislação penal e, especialmente, processual penal para acompanhar a evolução tecnológica.

Esses direcionamentos são importantes, pois o enfrentamento eficaz da criminalidade digital no Brasil exige uma abordagem sistêmica que integre três dimensões fundamentais: a legislação penal material, o arcabouço processual penal e as políticas públicas de Segurança Pública. A análise desenvolvida neste artigo demonstrou que a mera tipificação de condutas criminosas praticadas no ambiente virtual, embora necessária, revela-se insuficiente quando desacompanhada de instrumentos processuais adequados para a produção de provas digitais e de estruturas investigativas especializadas.

---

[38] Idem.

A legislação penal brasileira tem respondido ao fenômeno da criminalidade digital com a criação de tipos penais específicos e a qualificação de crimes tradicionais quando praticados por meio eletrônico. Contudo, essa expansão normativa não tem sido acompanhada por uma correspondente evolução do Direito Processual Penal, que permanece pautado por institutos concebidos para a realidade analógica. A ausência de regulamentação uniforme sobre a obtenção, preservação e valoração de provas digitais gera insegurança jurídica que compromete tanto a efetividade da persecução penal quanto a proteção de direitos fundamentais, especialmente a privacidade e a proteção de dados pessoais.

Por sua vez, a política de Segurança Pública brasileiro, historicamente centrada no policiamento ostensivo preventivo, não está estruturada para enfrentar as demandas investigativas complexas inerentes à criminalidade digital. A investigação de crimes cibernéticos exige investimento em capacitação técnica especializada, infraestrutura tecnológica adequada, cooperação interinstitucional e articulação internacional, elementos que permanecem deficitários na maioria das unidades federativas. A consequência dessa desarticulação é a perpetuação de elevados índices de impunidade, a dificuldade na descapitalização de organizações criminosas e o fortalecimento de redes criminosas difusas que operam predominantemente em ambiente digital.

Portanto, a eficácia no enfrentamento à criminalidade digital depende da construção de um sistema integrado que contemple: (a) legislação penal material que tipifique adequadamente as condutas lesivas praticadas no ambiente virtual; (b) arcabouço processual penal específico que regule uniformemente a produção de provas digitais, distinguindo dados em repouso, em trânsito e em processamento, com observância de garantias fundamentais e alinhamento a padrões internacionais; e (c) políticas públicas de Segurança Pública que priorizem a investigação criminal especializada, o investimento em tecnologia forense digital, a capacitação continuada de agentes públicos e a cooperação nacional e internacional.

Somente mediante essa integração sistêmica será possível superar a atual fragmentação normativa e operacional, promovendo maior segurança jurídica, eficiência na persecução penal e proteção efetiva dos bens jurídicos ameaçados pela criminalidade contemporânea. A realidade incômoda revelada por este estudo aponta para a urgência de uma reforma legislativa e institucional que reconheça a

especificidade da prova digital e adapte o sistema de justiça criminal às exigências do século XXI.

Da mesma forma, academicamente observando, ainda são necessários estudos empíricos sobre a eficácia das medidas legislativas penais e processuais penais e, especialmente, das medidas investigativas, tal qual como observado por Wendt[39]. Nesse caminho, pesquisas comparativas com modelos e políticas internacionais de persecução penal digital, para identificar boas práticas, são fundamentais.

Destaca-se, por fim, a importância da capacitação técnica e jurídica dos agentes públicos envolvidos na investigação e persecução penal digital, além da estruturação dos setores responsáveis, com a atenção devida pelos governos estaduais.

REFERÊNCIAS FINAIS

ASSOCIAÇÃO Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27037:2013** — Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2013.

BARRETO, Alesandro Gonçalves; WENDT, Emerson. **Inteligência e investigação criminal em fontes abertas**. 4.ª ed. Rio de Janeiro: Brasport, 2024.

BRASIL. **Lei n.º 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Seção 1.

BRASIL. **Lei n.º 13.968, de 26 de dezembro de 2019**. Altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), para modificar o crime de incitação ao suicídio e incluir as condutas de induzir ou instigar a automutilação, bem como a de prestar auxílio a quem a pratique. Diário Oficial da União, Brasília, DF, 27 dez. 2019, Seção 1, p. 2.

[39] WENDT, Emerson. **Investigação criminal cibernética no Brasil**: legislação, estrutura e desafios. Leme: Editora Mizuno, 2024.

BRASIL. **Lei n.º 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União, Brasília, DF, 24 dez. 2019, Seção 1, Edição Extra A, p. 1–7.
BRASIL. **Lei n.º 14.811, de 12 de janeiro de 2024**. Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares, prevê a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente e altera o Decreto-Lei n.º 2.848/1940, e as Leis nºs 8.072/1990 e 8.069/1990. Diário Oficial da União, Brasília, DF, 15 jan. 2024, Seção 1.

BRASIL. **Lei n.º 15.123, de 24 de abril de 2025**. Altera o art. 147-B do Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), para estabelecer causa de aumento de pena no crime de violência psicológica contra a mulher quando praticado com o uso de inteligência artificial ou de recurso tecnológico que altere imagem ou som da vítima. Diário Oficial da União, Brasília, DF, 25 abr. 2025, Seção 1, p. 3.

BRASIL. **Lei n.º 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei n.º 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Diário Oficial da União, Brasília, DF, 27 maio 2021, Edição extra nº 99-A, Seção 1.

BRASIL. **Lei n.º 13.718, de 24 de setembro de 2018**. Altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena e definir como causas de aumento o estupro coletivo e o estupro corretivo. Diário Oficial da União, Brasília, DF, 25 set. 2018, Seção 1, p. 2.

BRASIL. **Lei n.º 11.829, de 25 de novembro de 2008**. Altera a Lei n.º 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse desse material e outras condutas relacionadas à pedofilia na internet. Diário Oficial da União, Brasília, DF, 26 nov. 2008, Seção 1, p. 1.

BRASIL. **Lei n.º 9.605, de 12 de fevereiro de 1998**. Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências. Diário Oficial da União, Brasília, DF, 13 fev. 1998, Seção 1, p. 1, col. 1.

BRASIL. **Lei n.º 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, DF, 16 jul. 1990, Seção 1.

BRASIL. **Lei n.º 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990, Seção 1 (Suplemento), p. 1.

BRASIL. **Lei n.º 11.340, de 7 de agosto de 2006**. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher… Diário Oficial da União, Brasília, DF, 8 ago. 2006, Seção 1, p. 1, col. 1.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República.

BRASIL. **Lei n.º 13.022, de 8 de agosto de 2014**. Dispõe sobre o Estatuto Geral das Guardas Municipais. Diário Oficial da União, Brasília, DF, 11 ago. 2014, Seção 1 (Edição Extra), p. 1–3.

BRASIL. **Lei n.º 13.060, de 22 de dezembro de 2014**. Disciplina o uso dos instrumentos de menor potencial ofensivo pelos agentes de segurança pública, em todo o território nacional. Diário Oficial da União, Brasília, DF, 23 dez. 2014, Seção 1, p. 3, col. 1.

BRASIL. **Lei n.º 9.099, de 26 de setembro de 1995**. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Diário Oficial da União, Brasília, DF, 27 set. 1995, Seção 1, p. 15033.

BRASIL. **Lei n.º 7.210, de 11 de julho de 1984**. Institui a Lei de Execução Penal. Diário Oficial da União, Brasília, DF, 13 jul. 1984, Seção 1, p. 10227.

BRASIL. **Lei n.º 12.830, de 20 de junho de 2013**. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Diário Oficial da União, Brasília, DF, 21 jun. 2013, Seção 1, p. 1.

BRASIL. **Decreto-Lei n.º 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Diário Oficial da União, Brasília, DF, 13 out. 1941, Seção 1, p. 19699; retificação em 24 out. 1941, Seção 1, p. 20449.

BRASIL. **Lei n.º 9.296, de 24 de julho de 1996**. Regula a interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal. Diário Oficial da União, Brasília, DF, 25 jul. 1996, Seção 1.

BRASIL. **Lei n.º 12.850, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940; revoga a Lei n.º 9.034, de 3 de maio de 1995; e dá outras providências. Diário Oficial da União, Brasília, DF, 5 ago. 2013, Seção 1 (Edição Extra), p. 3.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014, Seção 1, p. 1.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018, Seção 1, p. 59; republicação na Edição Extra, 15 ago. 2018, p. 1.

BRASIL. **Lei Complementar nº 70, de 30 de dezembro de 1991**. Institui contribuição para financiamento da Seguridade Social, eleva a alíquota da contribuição social sobre o lucro das instituições financeiras e dá outras providências. Diário Oficial da União, Brasília, DF, 31 dez. 1991, Seção 1, p. 31057.

BRASIL. Ministério da Justiça e Segurança Pública. **Portaria n.º 855, de 17 de janeiro de 2025**. Regulamenta o Decreto nº 12.341, de 23 de dezembro de 2024, e estabelece diretrizes sobre o uso da força pelos profissionais de segurança pública. Diário Oficial da União, Brasília, DF, 17 jan. 2025, Seção 1 (Edição Extra), p. 2-4.

BRASIL. Senado Federal. **Projeto de Lei do Senado n.º 236, de 2012**. Reforma do Código Penal Brasileiro. Brasília, DF: Senado Federal, 2012. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/106404>. Acesso em: 21/09/2025.

BRASIL. Senado Federal. **Projeto de Lei do Senado n.º 156, de 2009**. Reforma do Código de Processo Penal. Brasília, DF: Senado Federal, 2009. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/90645>. Acesso em: 21/09/2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei n.º 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2326300>. Acesso em: 21/09/2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei n.º 4.143, de 2023**. Altera a Lei n.º 12.830, de 20 de junho de 2013, que dispõe sobre a investigação criminal conduzida pelo Delegado de Polícia. Brasília, DF: Câmara dos Deputados, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2382762>. Acesso em: 21/09/2025.

BRASIL. Conselho Nacional de Justiça. **Cidadania nos presídios**. Brasília, DF: CNJ, [s.d.]. Disponível em:<https://www.cnj.jus.br/sistema-carcerario/cidadania-nos-presidios/>. Acesso em: 21/09/2025.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus n. 372.762 – MG (2016/0254030-1)**. Rel. Min. Felix Fischer. 5ª Turma. Brasília, DF, j. 03 out. 2017. DJe 16 out. 2017. Disponível em: <https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?dt=20171016&formato=PDF&nreg=201602540301&seq=1631821&tipo=0>. Acesso em: 21/09/2025.

FÓRUM Brasileiro de Segurança Pública. **19º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: <https://publicacoes.forumseguranca.org.br/handle/123456789/279>. Acesso em: 21/09/2025.

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

INSTITUTO Sou da Paz. **Onde mora a impunidade?** Porque o Brasil precisa de um indicador nacional de esclarecimento de homicídios. 7. ed. São Paulo: Instituto Sou da Paz, 2024.

LUISI, Luiz. **Princípios constitucionais penais**. 2.ª ed. rev. e ampl. Porto Alegre: Sérgio Antonio Fabris Editor, 2003.

MENDRONI, Marcelo Batlouni**. Crime organizado**: aspectos gerais e mecanismos legais. 3.ª ed. São Paulo: Atlas, 2009.

PCI SECURITY STANDARDS COUNCIL. Payment Card Industry Data Security Standard (PCI DSS): **Requirements and Testing Procedures**. v. 4.0.1, jun. 2024. Disponível em: <https://www.pcisecuritystandards.org/document_library/>. (PCI DSS v4.0.1). Acesso em: 21/09/2025.

QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**,

São Paulo, v. 1, n. 1, p. 64–90, fev. 2020. Disponível em: <https://revista.internetlab.org.br/tercio-sampaio-ferraz-junior-e-sigilo-de-dados-o-direito-a-privacidade-e-os-limites-a-funcao-fiscalizadora-do-estado-o-que-permanece-e-o-que-deve-ser-reconsiderado/>. Acesso em: 21/09/2025.

ROXIN, Claus. **Estudos de Direito Penal**. 2.ª ed. rev. Tradução de Luís Greco. Rio de Janeiro: Renovar, 2008.

ROXIN, Claus. **A proteção de bens jurídicos como função do direito penal**. 2.ª ed. Organização e tradução de André Luís Callegari e Nereu José Giacomolli. Porto Alegre: Livraria do Advogado, 2009.

SHECAIRA, Sérgio Salomão. **Criminologia**. 6.ª ed. rev. e atual. São Paulo: Revista dos Tribunais, 2014.

UNITED STATES. **Electronic Communications Privacy Act of 1986 (ECPA)**. Public Law 99-508, 21 Oct. 1986. 100 Stat. 1848–1873. Washington, DC: U.S. Government Publishing Office, 1986. Disponível em: <https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1848>. Acesso em: 21/09/2025.

WENDT, Emerson. **Internet & Direito Penal**: risco e cultura do medo. Porto Alegre: Livraria do Advogado, 2017.

WENDT, Emerson. **As expectativas cognitivas e normativas dos atores de investigação policial em face dos crimes cibernéticos.** 2023. Tese (Doutorado em Direito) – Universidade LaSalle, Canoas, 2023.

WENDT, Emerson. **Investigação criminal cibernética no Brasil**: legislação, estrutura e desafios. Leme: Editora Mizuno, 2024.