REVISTA JURÍDICA DO MPRO

Ano 2025 nº especial
ISSN 2595-3265
Data de submissão: 16/09/2025
Data de Aprovação: 31/08/2025

A ausência de tipificação penal na Lei Geral Proteção de Dados: Desafios na persecução penal

The Absence of Criminal Typification in the General Data Protection Law: *Challenges for Criminal Prosecution*

Paulo Jonas Sales de Lima[1]

Felipe Magno Silva Fonsêca[2]

1 Graduado em Direito pela Faculdade Interamericana de Porto Velho, Pós-graduando em Políticas Públicas e Tutela dos vulneráveis pela Escola Superior do Ministério Público do Estado de Rondônia, Currículo Lattes: https://lattes.cnpq.br/2355995989290157. E-mail: paulojonas.sales@gmail.com.

2 Doutorando em Direito (PUC-PR). Mestre em Direito (UERJ). Especializações em: Proteção de Dados Pessoais: LGPD & GDPR (FMP); Direito Ambiental (EMERON); Direito Público (UNIDERP); Gestão Pública (UEPB); Investigação Digital (VINCIT - em curso). Graduação em Direito (UEPB). Data Protection Officer (DPO), com certificação internacional EXIN. Promotor de Justiça no MPRO. Coordenador de Proteção de Dados Pessoais do MPRO. Coordenador do Núcleo de Enfrentamento a Crimes Cibernéticos (NUCIBER-GAECO). Currículo Lattes: http://lattes.cnpq.br/4092677904013215. E-mail: 21855@mpro.mp.br.

Resumo

O presente trabalho analisa os limites da proteção jurídica conferida pela Lei Geral de Proteção de Dados (LGPD), especialmente diante da ausência de tipificação penal para condutas ilícitas envolvendo dados pessoais. A partir da constatação do crescimento exponencial de práticas como vazamentos, comercialização indevida e fraudes digitais, o estudo propõe uma reflexão sobre a suficiência dos instrumentos civis e administrativos previstos na LGPD e destaca os obstáculos enfrentados na persecução penal desses delitos. A pesquisa também examina propostas legislativas em curso que buscam criminalizar condutas graves relacionadas ao uso abusivo de dados, além de apontar a importância de políticas públicas voltadas à conscientização social sobre o tema. Conclui-se que a lacuna normativa compromete a efetividade da proteção dos dados pessoais no Brasil, sendo necessária uma abordagem multidimensional que integre sanção penal, educação digital e fortalecimento institucional.
Palavras-chave: LGPD; dados pessoais; tipificação penal; crimes digitais; cidadania digital.

Abstract

This paper analyzes the limitations of the legal protection provided by the Brazilian General Data Protection Law (LGPD), particularly in view of the absence of criminal offenses for illicit conduct involving personal data. Considering the exponential increase in practices such as data breaches, illegal trading, and digital fraud, the study reflects on the adequacy of the civil and administrative measures established by the LGPD and highlights the challenges faced by criminal prosecution in addressing such violations. It also examines ongoing legislative initiatives aimed at criminalizing serious misconduct related to the misuse of personal data, and emphasizes the importance of public policies focused on social awareness. The study concludes that the current normative gap undermines the effectiveness of data protection in Brazil, calling for a multidimensional approach that combines criminal sanctions, digital education, and institutional strengthening.
Keywords: LGPD; personal data; criminalization; cybercrime; digital citizenship.

Introdução

O direito à proteção dos dados pessoais passou a ocupar posição de destaque no ordenamento jurídico brasileiro, especialmente após a promulgação da Emenda Constitucional nº 115, em 10 de fevereiro de 2022. Todavia, destaca-se que a proteção normativa dos dados pessoais já se fazia presente anteriormente, por intermédio da Lei nº 13.709/2018, a chamada Lei Geral de Proteção de Dados (LGPD), a qual trouxe diretrizes claras e abrangentes sobre o tratamento de dados no Brasil.

Apesar do avanço normativo representado pela LGPD, observa-se que a legislação não contempla, em seu texto, a criminalização de condutas ilícitas envolvendo o uso indevido de dados pessoais. O legislador optou por concentrar as sanções nos âmbitos civil e administrativo, deixando lacuna importante no que se refere à responsabilização penal de indivíduos ou grupos que comercializam, manipulam ou utilizam indevidamente tais informações. Tal escolha enseja debates relevantes a respeito da suficiência da proteção atualmente oferecida.

Diante disso, questiona-se: a ausência de tipificação penal na LGPD enfraquece a proteção de dados no Brasil?

A partir dessa indagação, o foco central desta pesquisa consiste na análise da suficiência do arcabouço normativo vigente frente às crescentes práticas ilegais que envolvem o tratamento de dados pessoais.

A escolha deste objeto de estudo se justifica tanto por sua relevância jurídica quanto por seus reflexos sociais. Do ponto de vista jurídico, a discussão permite explorar os limites e as possibilidades do Direito Penal diante de novas demandas oriundas de uma sociedade movida à informação. Já no campo social, a abordagem contribui para a promoção da cidadania digital, fortalecendo a conscientização pública quanto à responsabilidade no uso de dados e à necessidade de um ambiente digital mais seguro e ético.

Dessa forma, o objetivo geral deste trabalho é analisar se a ausência de tipificação penal na LGPD enfraquece a proteção de dados no Brasil. Para alcançar tal meta, foram estabelecidos os seguintes objetivos específicos: (i) compreender o direito à proteção de dados pessoais e sua relevância na sociedade informacional; (ii) investigar os impactos práticos da ausência de tipos penais na responsabilização de condutas ilícitas no contexto da LGPD; e (iii) examinar se existem propostas legislativas ou discussões doutrinárias que visem à tipificação penal de condutas relacionadas ao uso indevido de dados pessoais.

A metodologia adotada será de natureza qualitativa, ancorada em pesquisa bibliográfica e documental. Serão consultados obras doutrinárias, artigos científicos, legislações nacionais e internacionais, além de projetos de lei e documentos institucionais. Complementarmente, recorre-se à análise de dados oriundos de órgãos oficiais, de modo a fundamentar a discussão.

No desenvolvimento do trabalho, o primeiro capítulo abordará os conceitos fundamentais relacionados aos dados pessoais, a trajetória normativa de sua proteção no Brasil e a evolução desse direito até sua constitucionalização. Em seguida, no segundo capítulo, será apresentada uma análise das limitações da LGPD quanto à ausência de tipos penais, bem como o uso de dispositivos penais genéricos atualmente aplicados de forma subsidiária. Por fim, o terceiro capítulo discutirá as propostas legislativas em curso que visam suprir essa lacuna normativa por meio da criação de tipos penais específicos para condutas que envolvam o tratamento indevido de dados pessoais.

1 A proteção de dados pessoais na sociedade da informação

Em breve contextualização sobre o termo sociedade da informação, é importante destacar que a expressão se consolidou por uso constante em âmbito político e normas oficiais adotadas por diversos países, a exemplo da Cúpula Mundial sobre a Sociedade da Informação (CMSI), organizada pela União Internacional de Telecomunicações (UIT), convocada pela Organização das Nações Unidas (ONU), a qual ocorreu em duas fases: Genebra em 2003, e Túnis, em 2005, eventos que deram notoriedade internacional ao conceito (Marques; Pinheiro, p.122, 2013).

Ademais, o mencionado termo remonta também ao Livro "O advento da sociedade pós-industrial" (1977) do sociólogo norte americano Daniel Bell, o qual aborda a sociedade da informação, descrevendo e antecipando as principais características da sociedade atual, ao dissertar que o conhecimento teórico e os serviços baseados no conhecimento se tornariam os alicerces da nova economia baseada na informação (Bell, 1977).

Nesse contexto, uma das preocupações que se destaca é o aumento da exposição dos dados pessoais. Com isso, direitos fundamentais como a privacidade, a dignidade da pessoa humana e o livre desenvolvimento da personalidade ficam cada vez mais vulneráveis e sujeitos a violações. Essa vulnerabilidade é característica do que Ulrich Beck denomina sociedade de risco, em que a modernidade produz novos tipos de ameaças que não podem ser totalmente controladas ou previstas (Beck, 2011).

A sociedade contemporânea é marcada pela ampla circulação de informação e conhecimento, tendo a revolução tecnológica e a globalização como fenômenos que impulsionam sua propagação.

De fato, a informação assume o papel central nas relações sociais, culturais, econômicas e políticas, tornando-se ativo estratégico tanto para empresas quanto para governos. Para Manuel Castells (1999), os dados tornaram-se não apenas um recurso técnico, mas um bem econômico e social de primeira ordem, sendo tratados como mercadorias valiosas.

A revolução tecnológica, aliada à evolução das Tecnologias da Informação e Comunicação (TICs), proporcionou a quebra de barreiras geográficas, permitindo conectar pessoas em tempo real por todo o globo, ou seja, essa conectividade gera novos desafios ao controle e à proteção da informação.

Neste viés, Manuel Castells (1999, p. 119-120) destaca a mudança de paradigma tecnológico, em que as novas tecnologias da informação se tornam mais flexíveis e poderosas, convertendo a própria informação em um produto moldável, distribuível e explorável economicamente.

Essa perspectiva crítica pode ser aprofundada sob a ótica da teoria sociológica de Zygmunt Bauman, em seu livro *Globalização: as consequências humanas* (1999), no qual disserta sobre a mobilidade do poder na era da globalização, vejamos:

> [..] Surge uma nova assimetria entre a natureza extraterritorial do poder e a contínua territorialidade da 'vida como um todo' — assimetria que o poder agora desarraigado, capaz de se mudar de repente ou sem aviso, é livre para explorar e abandonar às consequências dessa exploração. Livrar-se da responsabilidade pelas consequências é o ganho mais cobiçado e ansiado que a nova mobilidade propicia ao capital sem amarras locais, que flutua livremente (Bauman, 1999, p. 15-16).

A lógica descrita por Bauman se reflete na atual estrutura digital, em que Estados, plataformas e corporações circulam livremente com informações de bilhões de pessoas, enquanto os indivíduos seguem com pouca autonomia sobre sua exposição online, aceitam contratos de adesão, são monitorados constantemente e, quando há vazamentos ou abusos, arcam sozinhos com as consequências.

Esse cenário é analisado de forma contundente por Shoshana Zuboff (2021), ao apresentar o conceito de capitalismo de vigilância, no qual os dados pessoais deixam de ser apenas uma representação identitária e passam a funcionar como insumo central para modelos de negócio que se sustentam na previsão e indução de comportamentos futuros, ou seja, trata-se de uma nova lógica de acumulação, onde o valor não está mais na posse de bens materiais, mas na extração contínua de informações íntimas muitas vezes captadas sem o devido conhecimento ou consentimento dos titulares.

Nesse contexto, de modo complementar, diversos autores têm explorado o que se convencionou chamar de Estado de vigilância, expressão que designa a consolidação de formas de poder baseadas na captura e no controle da informação como recurso geopolítico.

Conforme apontado por Molinaro e Sarlet (2013, p. 67-70), a informação passa a circular como uma moeda assimétrica, sem equivalente direto em valor econômico tradicional, concentrando-se nas mãos de poucos Estados e corporações que detêm o "capital informacional" necessário para operar nesse novo mercado.

Assim, o poder assume feições invisíveis e onipresentes, sendo exercido não apenas pela coerção, mas pela observação constante, que atravessa fronteiras territoriais e penetra esferas antes consideradas privadas.

Portanto, essa dinâmica revela uma nova forma de desigualdade: a do controle e da responsabilidade sobre os dados pessoais, acentuando o desequilíbrio entre quem coleta e lucra com a informação e quem a fornece sem plena consciência ou consentimento real.

1.1 O direito à proteção de dados

O conceito de dado pessoal sofreu uma notável ampliação ao longo das últimas décadas. Atribui-se a origem do conceito às diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), publicadas em 23 de setembro de 1980, nas quais já se afirmava que dado pessoal consiste em toda informação vinculada a uma pessoa identificada ou identificável.

Esse conceito foi reafirmado em diversos documentos normativos no âmbito europeu. Em 1981, o Conselho da Europa o consolidou na Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal. Posteriormente, em 1995, o Parlamento Europeu reiterou a definição na Diretiva 95/46/CE.

Já em 2016, General Data Protection Regulation (GDPR), aprovado pelo regulamento do Parlamento Europeu nº 2016/679, trouxe uma definição mais precisa. Conforme o artigo 4º, item 1, considera-se dado pessoal "qualquer informação relativa a uma pessoa física identificada ou identificável". Além disso, o GDPR esclarece o termo "identificável", conforme se observa:

> [..] Considera-se identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular (União Europeia, 2016).

No Brasil, a LGPD incorporou esse mesmo entendimento. Conforme o art. 5º, inciso I, dado pessoal é "informação relacionada a pessoa natural identificada ou identificável". Registre-se que a lei distingue os chamados dados pessoais sensíveis, nos termos do inciso II, do mesmo artigo, como aqueles referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, sempre vinculados a uma pessoa natural (Brasil, 2018).

Dessa forma, observa-se que os dados pessoais assumem contornos jurídicos específicos que os diferenciam de outras informações. Conforme ensina Danilo Doneda (2006), os dados pessoais não se resumem a elementos técnicos ou estatísticos, eles expressam características únicas da pessoa a que se referem e, por isso, são componentes da sua personalidade jurídica.

Nesse mesmo sentido, Mendes e Doneda (2016, p. 3) afirmam que os dados pessoais "não devem ser tutelados por seu valor instrumental, mas sim pela sua vinculação direta à identidade do sujeito". Assim, a proteção jurídica se impõe não pelos dados em si, mas pela centralidade que eles ocupam na construção da identidade e da autonomia do titular.

Portanto, em face da crescente relevância dos dados na sociedade informacional e da sua vinculação direta à esfera privada dos indivíduos, a proteção de dados tornou-se elemento indispensável à garantia dos direitos fundamentais.

1.2 Contexto da regulação nacional: A Lei Geral de Proteção de Dados

No âmbito nacional, o processo de consolidação normativa da proteção de dados se desenvolveu de maneira tardia e fragmentada, sobretudo se comparado a ordenamentos estrangeiros que já avançavam rumo a uma cultura jurídica mais robusta. Como pontua Fonseca (2023, p. 73), mesmo diante da ausência de uma legislação específica nas primeiras décadas, o ordenamento constitucional brasileiro já trazia dispositivos capazes de amparar, ainda que

indiretamente, a proteção de dados pessoais, a liberdade de expressão, a inviolabilidade das comunicações e a privacidade.

Nesse contexto, no plano infraconstitucional, diversas legislações anteciparam preocupações normativas que, embora não organizadas sob o paradigma da proteção de dados, refletiam certa sensibilidade ao tema. O Código de Defesa do Consumidor (Lei nº 8.078/1990), a Lei do Habeas Data (Lei nº 9.507/1997), a Lei do Cadastro Positivo (Lei nº 12.414/2011), a Lei de Acesso à Informação (Lei nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965/2014) são exemplos paradigmáticos dessa movimentação normativa dispersa.

O Código de Defesa do Consumidor, conforme destaca Fonseca (2023, p. 77), foi um dos primeiros a reconhecer a hipervulnerabilidade informacional do cidadão consumidor, impondo limites à manipulação de dados por meio da exigência de correção, finalidade e transparência no uso de cadastros. Todavia, seu campo de incidência limitado às relações de consumo impediu que se firmasse como uma matriz normativa de aplicação ampla. Ou seja, sua eficácia se via condicionada à lógica contratual-consumerista, o que, por si só, já restringia seu alcance social e regulatório.

Por sua vez, o Marco Civil da Internet emerge como resposta política e jurídica a uma conjuntura internacional marcada pela revelação, por Edward Snowden, dos mecanismos de vigilância em massa promovidos pelos Estados Unidos e empresas transnacionais. Segundo Fonseca (2023, p. 79), a Lei nº 12.965/2014 representou um avanço ao consagrar princípios como liberdade de expressão, proteção da privacidade e segurança de dados no uso da internet.

A mencionada lei, em seus art. 3º e 7º, consagrou a tentativa de institucionalizar uma arquitetura mínima de direitos digitais, incluindo o direito à exclusão de dados, ao consentimento expresso e à informação clara sobre o tratamento de dados pessoais, contudo, ainda operava de forma fragmentária e não dava conta da multiplicidade de atores e práticas que extrapolam o ambiente virtual.

Nesse cenário, a promulgação da LGPD não apenas representa uma mudança de direção, mas também uma tentativa de unificação e de sistematização dos esforços anteriores, que assume contornos constitucionais mais robustos com a Emenda Constitucional nº 115/2022.

Assim, a LGPD não nasce de forma isolada, mas com a culminância de um processo legislativo complexo, multifacetado e atravessado por pressões externas e internas. Conforme lecionam Bioni e Rielli (2021, p. 32), ao discorrerem sobre os principais vetores que impulsionaram sua aprovação, destaca-se o escândalo da empresa Cambridge Analytica, a vigência do GDPR europeu, as exigências internacionais impostas ao Brasil para ingresso na OCDE e a articulação interna em torno da regulamentação do Cadastro Positivo. Assim, a LGPD nasce como reflexo da interdependência entre o local e o global, entre soberania regulatória e alinhamento internacional.

Além disso, a lei incorpora princípios estruturantes como finalidade, necessidade, transparência, segurança e responsabilização, além de instituir a criação de mecanismos institucio-

nais como a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados e da Privacidade (CNPD), sendo a ANPD, uma autarquia de regime especial, responsável pela tutela dos dados pessoas e pela aplicação de sanções de cunho administrativo e cível.

Em síntese, embora o percurso brasileiro tenha sido marcado por avanços normativos pontuais e desarticulados, a promulgação da LGPD representa um salto qualitativo significativo, apto a dialogar com os desafios contemporâneos da sociedade digital e a firmar, ainda que tardiamente, um compromisso público com a dignidade informacional do cidadão.

2 A ausência de tipificação penal na LGPD e seus reflexos na persecução penal

A proteção jurídica dos dados pessoais no Brasil tem sido conduzida pelas esferas civil e administrativa, todavia, observa-se que tais mecanismos, embora necessários, não se mostram suficientes para resguardar de forma eficaz um bem jurídico de natureza tão sensível quanto os dados pessoais.

Conforme descreve Sydow (2022), essa insuficiência revela-se, sobretudo, na incapacidade de conter práticas sistemáticas de violação, notadamente em contextos marcados pela criminalidade organizada e pelo comércio clandestino de informações, ou seja, a legislação infraconstitucional, ainda que represente um avanço, não tem alcançado os casos mais graves de exposição e manipulação indevida de dados.

Nesse sentido, a globalização econômica, o consumo desmedido, os riscos ambientais e o avanço da criminalidade transnacional impõem desafios complexos ao Estado. Aliás, como observa Brito (2013), esse cenário contribui para a adequação do Direito Penal como instrumento de contenção de novas formas de ameaça.

É cediço que o Direito Penal, além de proteger bens jurídicos, cumpre uma função preventiva. Aliás, se desconsiderarmos essa finalidade não se sustentaria a sua legitimidade em um Estado Democrático de Direito. Na prática, percebe-se que o modelo penal clássico não atua de forma antecipada, mas apenas posteriormente à lesão, punindo o resultado danoso já consumado. Importa frisar que, diante dessa lógica reativa, cresce o clamor por uma proteção penal eficaz e preventiva, especialmente no que se refere aos dados pessoais (Brito, 2013).

A responsabilização penal, nesse contexto, possui a missão de proteger bens jurídicos essenciais à convivência ordenada em sociedade. Dessa forma, atua como um instrumento de última instância, sendo convocada apenas quando os demais ramos do Direito se mostram ineficazes. Segundo prelecionam Souza e Japiassú (2018, p. 121), essa intervenção mínima pressupõe que apenas bens de elevada relevância social devem justificar o uso da sanção penal. Sob essa ótica, os dados pessoais, por sua relação direta com a dignidade da pessoa humana, se enquadram como objetos legítimos de tutela penal.

Roxin (2006, p. 39) corrobora essa perspectiva ao afirmar que da dignidade humana decorre a proibição de se instrumentalizar o ser humano, o que se aplica diretamente ao tratamento indevido de dados. Ou seja, ao permitir o uso indevido dessas informações, admite-se uma forma contemporânea de domínio sobre a identidade e a vontade do indivíduo. Cabe destacar que, nesse cenário, os dados não são apenas um patrimônio ou recurso informacional, mas sim uma extensão da individualidade.

Hassemer (2011) reforça essa análise ao apontar que os bens jurídicos penais são definidos não apenas teoricamente, mas também pela prática social e pela percepção dos riscos. Nesse sentido, a frequência das violações e a gravidade dos danos decorrentes do uso indevido de dados pessoais indicam, por si só, a necessidade de uma resposta penal proporcional. Assim, pode-se inferir, que a realidade social demanda um novo olhar sobre a proteção penal desse bem jurídico.

Por fim, a elevação da proteção de dados pessoais ao status de direito fundamental (CF, art. 5º, LXXIX), aliada à recente adesão do Brasil à Convenção de Budapeste, evidencia como uma clara tendência normativa e internacional a construção de uma tutela penal robusta e estruturada.

2.1 Dificuldades práticas na persecução penal

A ausência de previsão de crimes específicos sobre dados pessoais redunda na problemática de limitação dos tipos penais existentes, já que as condutas em que os dados pessoais poderiam figurar o bem jurídico protegido apenas são interpretadas como conduta meio (Brito, 2013).

O art. 52 da LGPD dispõe sobre sanções aplicáveis em caso de infrações às suas normas, destacam-se: advertência, com indicação de prazo para adoção de medidas corretivas, multa simples, multa diária, bloqueio dos dados pessoais e eliminação dos dados pessoais relacionados à infração, entre outras. Tais sanções têm caráter administrativo, porém resguardando do direito de pleitear danos no âmbito cível, e visam promover o cumprimento da norma por meio de mecanismos de controle (Brasil, 2018).

Apesar da diversidade de sanções, não há previsão de tipos penais na LGPD. Assim, condutas como a comercialização indevida de dados, o vazamento proposital de informações sensíveis ou o uso de dados para fraudes eletrônicas não encontram, na própria LGPD, instrumentos penais de repressão direta, o que obriga o intérprete a buscar amparo em tipos penais genéricos.

Nesse contexto, a responsabilização administrativa busca corrigir condutas e evitar reincidências, sem, contudo, possuir força intimidatória suficiente para desestimular práticas dolosas e reiteradas. A responsabilização civil, por sua vez, tem como objetivo a reparação de danos, mas é de caráter individual e exige prova do prejuízo causado, o que pode ser de difícil comprovação.

Um dos tipos penais mais utilizados em casos de violação de dados é o artigo 154-A do Código Penal, que trata da invasão de dispositivo informático. Contudo, essa tipificação mos-

tra-se limitada, pois exige o uso de meio indevido para o acesso e não abarca situações em que o dado é obtido legalmente e depois reutilizado de maneira abusiva. Além disso, não contempla condutas como a venda ou compartilhamento não autorizado de dados pessoais (Sydow, 2022).

A persecução penal de crimes informáticos e relacionados à proteção de dados encontra múltiplos obstáculos. Em primeiro lugar, trata-se de crimes complexos, que envolvem redes anônimas, estruturas transnacionais e uso avançado de tecnologias, dificultando a identificação dos autores e a obtenção de provas (Sydow, 2022).

A ausência de tipificação penal na LGPD reflete uma omissão legislativa e perda de oportunidade diante de uma realidade tecnológica em constante transformação, já que o aumento de crimes digitais envolvendo dados pessoais, como fraudes financeiras, extorsões e comercialização de informações sensíveis, evidencia a necessidade de modernizar o sistema penal para enfrentar essas novas ameaças (Sydow, 2022).

Portanto, essa lacuna normativa não apenas enfraquece a proteção jurídica dos titulares de dados, como também compromete a credibilidade institucional do sistema de proteção de dados. A criminalização de condutas graves deve ser debatida com responsabilidade e equilíbrio, sem incorrer em um punitivismo excessivo, mas com a construção de um marco legal mais coerente com os riscos da sociedade informacional.

2.2 Panorama atual de violações e vulnerabilidades

Atualmente, o cenário nacional evidencia que o tratamento de dados pessoais ainda é permeado por fragilidades, conforme evidenciam os recorrentes casos alarmantes de vazamentos e incidentes de segurança que atingem milhões de titulares e colocam em xeque a efetividade das normas de proteção existentes.

Um dos episódios mais emblemáticos ocorreu em janeiro de 2021, quando vieram a público informações sobre o maior vazamento de dados da história brasileira, com exposição de dados de 223 milhões de pessoas, incluindo indivíduos já falecidos. As informações vazadas incluíam nome completo, CPF, endereço, telefone, salário, score de crédito, dados de veículos e até vínculos familiares, sendo atribuída a origem à base de dados da Serasa Experian (Castro, 2021).

Na mesma linha, o sistema do Ministério da Saúde sofreu ataque hacker em dezembro de 2021, que resultou na indisponibilidade do Conecte SUS e no apagamento de registros de vacinação contra a COVID-19, afetando diretamente a continuidade de políticas públicas de saúde (G1, 2021).

Dessa forma, é possível perceber que os principais tipos de vulnerabilidade identificados envolvem desde a ausência de criptografia e falhas em políticas de consentimento, até a inexistência de mecanismos eficazes para a revogação do tratamento de dados por parte dos titulares. Tais fatores revelam não apenas a fragilidade estrutural de sistemas públicos e privados, mas também a carência de uma cultura de proteção de dados consolidada no país.

Além das falhas técnicas e de gestão, é necessário destacar o papel da desinformação e da ausência de políticas públicas voltadas à educação digital da população, já que a baixa familiaridade de muitos brasileiros com os direitos previstos na LGPD contribui para que a responsabilização de agentes infratores seja limitada e, muitas vezes, ineficaz.

Portanto, verifica-se que as violações à proteção de dados no Brasil não são casos isolados, mas reflexos de uma estrutura normativa e institucional ainda em processo de amadurecimento. Logo, a ausência de responsabilização penal adequada e a inexistência de mecanismos de dissuasão eficazes reforçam a necessidade de avanços legislativos, educativos e institucionais.

3 Propostas legislativas e políticas públicas para a proteção penal de dados pessoais

A crescente fragilidade da proteção de dados frente a condutas ilícitas complexas, torna imprescindível a adoção de medidas legislativas e institucionais que reforcem a efetividade da LGPD, não apenas por meio de propostas de reforma penal, mas também com a implementação de políticas públicas voltadas à conscientização social e à inclusão digital dos grupos mais vulneráveis.

O tópico a seguir visa uma análise dos projetos de lei que circundam o ordenamento jurídico brasileiro, em razão da omissão do legislador em editar lei específica para regular os limites do tratamento de dados pessoais pelas forças de segurança pública, conforme dispõe o art. 4º, inciso III, da LGPD.

3.1 Análise do anteprojeto de lei de proteção de dados para a segurança pública

Um dos atos legislativos mais expressivos sobre o tema consistiu no Ato do Presidente nº 58.133, de 26 de novembro de 2019, que institui a Comissão de Juristas destinada à criação de um anteprojeto de lei voltado especificamente à proteção de dados no contexto penal e de segurança pública (Brasil, 2019).

O Projeto de Lei nº 1515/2022, de iniciativa do Deputado Federal Coronel Armando, visa instituir uma legislação específica sobre proteção de dados no âmbito da segurança pública e da persecução penal. Trata-se, pois, de uma proposta que regulamenta o tratamento de dados pessoais realizado por autoridades competentes para fins de segurança do Estado, defesa nacional, segurança pública e atividades de investigação e repressão de infrações penais (Brasil, 2022).

Em paralelo, o instituto Legal Grounds for Privacy Design (LGPD) em parceria com a Escola Superior do Ministério Público da União (ESMPU), realizou encontros virtuais com juristas, acadêmicos e especialistas sobre a temática de criação da LGPD Penal. Nesse caso, vale ressaltar o documento denominado “exposição de motivos”, que destaca premissas sobre anteprojeto, cuja minuta inicial foi apresentada, diferenciando-se do PL nº 1515/2022, ao passo em

que reconhece expressamente a proteção de dados pessoais como bem jurídico penal, propondo, inclusive, a criminalização da transmissão indevida dessas informações (ESMPU, 2021).

Ademais, sugere a inserção, no Código Penal, do capítulo V – Dos Crimes contra a Proteção de Dados Pessoais, prevendo o tipo penal de transmissão ilegal de dados pessoais, nos seguintes termos:

> Art.154-C.**Transmitir, distribuir, usar de forma compartilhada, transferir, comunicar, difundir dados pessoais ou interconectar bancos de dados pessoais sem autorização legal para obter vantagem indevida ou prejudicar o titular dos dados ou terceiro a ele relacionado**: pena – reclusão de 1 (um) a 4 (quatro) anos e multa. Aumenta-se a pena de um a dois terços se os dados forem sensíveis ou sigilosos, ou se o crime for cometido por funcionário público em razão do cargo (ESMPU, 2021, s/p, grifo nosso).

O anteprojeto elaborado pela comissão de juristas avança em relação ao PL nº 1515/2022 ao propor a criminalização da transmissão indevida de dados e ao reconhecer a proteção de dados como bem jurídico penal. Assim, a proposta preenche lacunas da LGPD, trazendo maior segurança jurídica e instrumentos mais eficazes para o enfrentamento das condutas ilícitas.

Em resumo, a criação de tipos penais específicos é medida necessária para fortalecer a resposta do sistema de justiça frente às infrações penais relacionadas ao uso indevido de dados pessoais. A atualização da legislação penal representa um passo essencial para proteger os dados e garantir maior efetividade na responsabilização dessas condutas.

3.2 Políticas públicas para conscientização social

A elaboração de políticas públicas voltadas à conscientização da sociedade sobre a importância dos dados pessoais é essencial para que o cidadão compreenda seus direitos e deveres, bem como saiba como exercê-los na prática.

A internet, por sua vez, desponta como uma ferramenta poderosa para o desenvolvimento econômico e social. Todavia, ela também inaugurou novas formas de interação social, inclusive gerando novos atritos e abrindo espaço para uma zona criminógena até então inexistente (Brito, 2013).

Nesse contexto, como bem observa Brito (2013), a prevenção é de suma importância para combater a criminalidade informática, visto que a busca por inclusão digital sem a devida cautela acabou se tornando um dos fatores que impulsionaram o crescimento dessas incidências, muito por conta do despreparo e da falta de conhecimento por parte da população.

Diante disso, vale ressaltar a teoria de mobilização de viés, a qual destaca que a formulação de uma política pública deriva de conflitos explorados por organizações políticas que podem se expandir e se transformar em uma questão política (Schattschneider, 1960, p. 71, *apud* Capella, 2018, p.16).

A mencionada teoria tem como pressuposto a ideia de que determinados conflitos são mais vistosos, logo tendem a serem promovidos em detrimento de outros, portanto, cabe aos atores políticos promover seus conflitos, a fim de mobilizarem atenção e obterem engajamento da sociedade (Schattschneider, 1960, p.71, apud Capella, 2018, p.17).

Com esse cenário posto, observa-se que a temática da proteção de dados pessoais ainda não tem conseguido se projetar como um conflito politicamente visível. Isso se deve, em grande medida, à baixa mobilização dos atores sociais diretamente afetados, bem como à dificuldade de articulação política em torno da pauta. Se não houver pressão significativa da sociedade civil ou de grupos organizados, o tema permanece restrito a nichos técnicos e jurídicos, sem alcançar o debate público mais amplo.

Assim, conforme propõe a teoria da mobilização de viés, a ausência de conflito visível limita sua transformação em prioridade na formulação de políticas públicas.

Importa frisar que medidas como a inclusão da proteção de dados nos currículos escolares, a capacitação de agentes públicos, o incentivo a campanhas de mídia sobre boas práticas digitais e a promoção de fóruns participativos sobre privacidade são essenciais para construção de uma cultura que valorize e respeite a informação pessoal.

Por conseguinte, pode-se argumentar que a eficácia da tutela penal dos dados pessoais está diretamente atrelada ao fortalecimento das instituições, ao aprimoramento técnico das estruturas de investigação e julgamento, bem como à formação de uma consciência social crítica.

Considerações finais

Ao longo desta pesquisa, buscou-se compreender os desafios da proteção de dados pessoais no Brasil a partir da ausência de tipos penais na LGPD. No primeiro capítulo, foram abordadas as transformações sociais provocadas pela sociedade da informação e os riscos emergentes desse novo paradigma, sob o ponto de vista da exposição crescente dos dados, impulsionada pela lógica de mercado e pela circulação global de informações.

Nessa análise, autores como Daniel Bell, Zuboff, Ulrich Beck e Zygmunt Bauman ofereceram importantes contribuições para entender o contexto da chamada sociedade da informação e os riscos que dela decorrem.

No segundo capítulo, concentrou-se a atenção nas limitações práticas da LGPD em lidar com infrações graves. Ainda que a norma represente um avanço significativo, ela se mostra insuficiente quando o assunto é responsabilização penal.

O fato de a legislação atual não prever crimes específicos relacionados ao uso indevido de dados gera uma série de dificuldades na persecução penal, especialmente diante da complexidade dos crimes cibernéticos. A jurisprudência acaba recorrendo a dispositivos genéricos, como o artigo 154-A do Código Penal, que muitas vezes não abrangem o núcleo da conduta ilícita, revelando uma lacuna normativa relevante.

Já no terceiro capítulo, foram analisadas propostas legislativas em andamento, como o Projeto de Lei nº 1515/2022 e o anteprojeto elaborado pela Comissão de Juristas, que pretende instituir crimes específicos voltados à proteção de dados pessoais.

Além do debate jurídico, discutiu-se a necessidade de políticas públicas que promovam maior conscientização sobre o tema, algo essencial num país que ainda engatinha em termos de educação digital. À luz da teoria da mobilização de viés, observou-se que a falta de visibilidade política do tema contribui para sua lenta evolução legislativa, o que indica a necessidade de maior pressão social e institucional.

Diante dos elementos analisados, é possível afirmar que a ausência de tipos penais na LGPD compromete a efetividade da proteção dos dados pessoais no Brasil, sobretudo diante do crescimento de práticas ilícitas sofisticadas que envolvem o tratamento e a comercialização indevida dessas informações. Os instrumentos cíveis e administrativos, embora relevantes, não têm apresentado força suficiente para coibir ou punir devidamente os responsáveis por essas práticas, o que evidencia uma fragilidade estrutural no modelo normativo atual.

Em síntese, uma possível saída seria a formulação de uma legislação penal específica, que tipifique condutas graves de forma proporcional e adequada à realidade digital contemporânea. Contudo, essa não deve ser a única resposta, visto que a construção de um sistema protetivo eficaz também passa por ações educativas, fortalecimento institucional, investimentos em investigação cibernética e, principalmente, por uma cultura que valorize a privacidade como direito fundamental, e não apenas como um detalhe técnico ou contratual.

Referências

BAUMAN, Zygmunt. **Globalização**: as consequências humanas. Tradução Marcus Penchel. Rio de Janeiro: Zahar, 1999.

BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. Tradução Sebastião Nascimento. 2. ed. São Paulo: Editora 34, 2011.

BELL, Daniel. **O advento da sociedade pós-industrial**. São Paulo: Cultrix, 1977.

BIONI, B. R.; RIELLI, M. M. A construção multissetorial da LGPD: história e aprendizados. In: BIONI, B. R. (org.). **Proteção de dados: contexto, narrativas e elementos fundantes**. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021. p. 31-54. Disponível em: https://brunobioni.com.br/livros/protecao-de-dados/. Acesso em: 23 jun.2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 abr. 2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1.515, de 2022**. Dispõe sobre o tratamento de dados pessoais para fins de segurança pública e persecução penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300. Acesso em: 15 abr. 2025.

BRASIL. Câmara dos Deputados. **Ato do Presidente nº 58.133, de 26 de novembro de 2019**. Institui Comissão de Juristas destinada à elaboração de proposição legislativa para regulamentar o art. 4º, §1º, inciso II, alínea "d" da Lei nº 13.709, de 14 de agosto de 2018 (LGPD). Disponível em: https://www2.camara.leg.br/legin/int/atoprt_sn/2019/atodopresidente-58133-26-novembro-2019-789470-publicacaooriginal-159494-cd-presi.html. Acesso em: 1 jun. 2025.

BRASIL. **Decreto nº 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. Brasília, DF, 13 abr. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm.Acesso em: 14 abr. 2025.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal.Brasília, DF, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 14 abr. 2025.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**.Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 14 abr. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 abr. 2025.

BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2013.

CAPELLA, Ana Cláudia Niedhardt**. Formulação de políticas públicas**. Brasília: Escola Nacional de Administração Pública, 2018. Disponível em: https://repositorio.enap.gov.br/bitstream/1/3332/1/Livro_Formula%C3%A7%C3%A3o%20de%20pol%C3%ADticas%20p%C3%BAblicas.pdf. Acesso em: 25 jun. 2025.

CASTELLS, Manuel. **A era da informação**: economia, sociedade e cultura – A sociedade em rede. v. 1. 6. ed. São Paulo: Paz e Terra, 1999.

CASTRO, Luiz Felipe. Maior vazamento de dados pessoais do país expõe riscos da era digital. **Veja**, São Paulo, 2021. Disponível em: https://veja.abril.com.br/tecnologia/maior-vazamento-de-dados-pessoais-do-pais-expoe-riscos-da-era-digital/. Acesso em: 02 jun. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da disciplina no contexto da informação. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 10 set. 2025.

FONSECA, Felipe Magno Silva**. Tutela penal dos dados pessoais na sociedade informacional de riscos**. 2023. 152 f. Dissertação (Mestrado em Direito) – Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2023. Disponível em: https://www.bdtd.uerj.br:8443/bitstream/1/21519/2/Disserta%C3%A7%C3%A3o%20-%20Felipe%20Magno%20Silva%20Fonseca%20-%202023%20-%20Completa.pdf. Acesso em: 25 jun. 2025.

JORNAL NACIONAL. Ministério da Saúde sofre ataque hacker e tem dados vacinais apagados. **G1**, 10 dez. 2021. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2021/12/10/ataque-hacker-ao-site-do-ministerio-da-saude-tira-do-ar-o-conectesus.ghtml. Acesso em: 16 abr. 2025.

HASSEMER, Winfried. Linhas gerais de uma teoria pessoal do bem jurídico. In: GRECO, Luís; TÓRTIMA, Fernanda Lara. (org.) et. al. **O bem jurídico como limitação do poder estatal de incriminar?** Rio de Janeiro: Lumen Juris, 2011. p. 22-23.

JAPIASSÚ, Carlos Eduardo Adriano. **Direito Penal**. Volume único. São Paulo: Atlas, 2018. E-book.

MARQUES, Lilian Emanueli; PINHEIRO, Marta Macedo Kerr. A Cúpula Mundial sobre a Sociedade da Informação: foco nas políticas de informação. **Inf. & Soc.: Est.**, João Pessoa, v.23, n.1, p. 117-131, jan./abr. 2013. p. 122).Disponível em: https://periodicos.ufpb.br/index.php/ies/article/view/15450/9536. Acesso em: 16 abr. 2025.

MINISTÉRIO PÚBLICO DA UNIÃO. **Exposição de motivos sobre o anteprojeto da LGPD Penal**. Disponível em: https://escola.mpu.mp.br/a-escola/comunicacao/noticias/especialistas-discutem-anteprojeto-da-lgpd- penal/anteprojeto-lgpd-penal.pdf/view. Acesso em: 28 abr. 2025.
OCDE. **Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data**. 2013. p. 13. Disponível em: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. Acesso em: 29 jun.2025.

SCHERTEL MENDES, Laura; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. **Revista de Direito Civil Contemporâneo , [S. l.]**, v. 9, p. 35–48, 2017. Disponível em: https://ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/171. Acesso em: 10 set. 2025.

ROXIN, Claus. **Estudos de Direito Penal**. Tradução de: Luís Greco. Rio de Janeiro: Renovar, 2006. p. 39.

SYDOW, Spencer Toth. **Curso de direito penal informático**. 3. ed. Salvador: Editora JusPodivm, 2022.

UNIÃO EUROPEIA. **Convenção nº 108, de 28 de janeiro de 1981**. Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal. Disponível em: https://rm.coe.int/1680078b37. Acesso em: 23 jun.2025.

UNIÃO EUROPEIA. **Regulamento nº 2016/679, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 24 jun.2025.

UNIÃO EUROPEIA. **Directiva nº 95/46/CE, de 24 de outubro de 1995**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046. Acesso em: 30 jun.2025.

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