

Entre a Privacidade e o Cibercrime: A Insuficiência Penal na Era dos Dados

Between Privacy and Cybercrime: Criminal Law Inadequacy in the Data Age

Kelly Beatriz Sousa do Nascimento

Khayam Ramalho da Silva Sousa

RESUMO

A expansão exponencial das tecnologias digitais, ao mesmo tempo em que reconfigura as dinâmicas sociais e econômicas, catalisa a proliferação dos crimes cibernéticos, impondo desafios críticos ao sistema penal tradicional. O presente artigo investiga em que medida a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) opera como um instrumento estratégico na prevenção e repressão das condutas criminosas digitais e identifica os principais obstáculos de sua aplicação no âmbito penal, notadamente na tipificação, investigação e sanção dos delitos. Metodologicamente, o estudo é fundamentado em uma revisão bibliográfica narrativa e doutrinária, consultando bases científicas especializadas como SciELO e Google Acadêmico. Os resultados evidenciam que, embora a LGPD constitua um avanço normativo essencial para a proteção da privacidade, sua contribuição à repressão penal é severamente limitada pela ausência de tipificações específicas no Código Penal e pela complexidade transnacional dos ambientes virtuais. Conclui-se que a tutela penal dos dados pessoais exige uma reforma sistêmica, demandando o desenvolvimento de instrumentos legais mais robustos, o investimento maciço em capacitação institucional dos operadores do Direito e o urgente fortalecimento da cooperação jurídica internacional para o combate eficaz aos crimes cibernéticos.

Palavras-chave: LGPD. Crimes Cibernéticos. Direito Penal Digital. Privacidade digital.

ABSTRACT

The exponential expansion of digital technologies, while reconfiguring social and economic dynamics, catalyzes the proliferation of cybercrime, imposing critical challenges to the traditional penal system. This article investigates to what extent the General Personal Data Protection Law (Law No. 13,709/2018) operates as a strategic instrument in preventing and repressing digital criminal conduct and identifies the main obstacles to its application in the criminal sphere, notably in the typification, investigation, and sanctioning of crimes. Methodologically, the study is based on a narrative and doctrinal bibliographic review, consulting specialized scientific databases such as SciELO and Google Scholar. The results show that, although the LGPD constitutes an essential normative advance for privacy protection, its contribution to criminal repression is severely limited by the absence of specific typifications in the Penal Code and the transnational complexity of virtual environments. It is concluded that the criminal protection of personal data requires a systemic reform, demanding the development of more robust legal instruments, massive investment in institutional capacity-building for legal operators, and the urgent strengthening of international legal cooperation to effectively combat cybercrime.

Keywords: LGPD. Cybercrime. Digital Criminal Law. Digital Privacy.

1. Introdução

O avanço das tecnologias digitais, somado à crescente dependência das interações mediadas pela internet, trouxe inúmeros benefícios à sociedade contemporânea, mas também deu origem a novas e sofisticadas formas de criminalidade. Os crimes cibernéticos, caracterizados por condutas que utilizam sistemas informáticos como meio ou fim ilícito,

apresentam desafios exponenciais para o direito penal, sobretudo no que se refere à proteção da privacidade e da segurança dos dados pessoais. Nesse contexto, a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representou um marco regulatório essencial no Brasil, buscando alinhar o ordenamento jurídico nacional às tendências internacionais de tutela da privacidade (Silva; Novais, 2023).

A LGPD surgiu como resposta à necessidade de disciplinar a coleta, o armazenamento e o uso de informações pessoais em meio digital, visando garantir maior controle por parte dos titulares dos dados. Contudo, essa mesma centralidade dos dados pessoais os transformou em alvo prioritário de criminosos, que exploram vulnerabilidades tecnológicas para a prática de condutas ilícitas. O aumento da incidência de fraudes eletrônicas, invasões de sistemas e vazamentos de informações sensíveis expõe a fragilidade da proteção, revelando uma lacuna crítica entre a legislação de proteção de dados e a efetiva capacidade do direito penal em reprimir essas práticas (Damião; Novais, 2024).

Essa criminalidade digital é marcada pela complexidade técnica e pela transnacionalidade das condutas, o que impõe obstáculos significativos à investigação e à persecução penal. A própria tipificação de muitos delitos ainda não acompanha a vertiginosa evolução tecnológica, havendo situações em que a aplicação do Código Penal Brasileiro se mostra insuficiente para enquadrar adequadamente determinadas práticas ilícitas (Zacarias; Freire, 2023).

Dessa forma, tal dissonância levanta questionamentos urgentes sobre a necessidade de criação de novos tipos penais específicos, capazes de conferir maior segurança jurídica e eficácia no combate às infrações digitais. A proteção de dados pessoais, alçada à condição de direito fundamental, reforça a importância de uma abordagem penal que seja compatível com as diretrizes da LGPD, mas enfrenta dificuldades práticas de implementação, tanto na esfera administrativa (ANPD) quanto na esfera penal.

Diante desse panorama, o presente artigo busca responder à seguinte pergunta de pesquisa: Em que medida a Lei Geral de Proteção de Dados Pessoais (LGPD) contribui para a prevenção e repressão dos crimes cibernéticos, e quais são os principais desafios de sua aplicação no âmbito penal, especialmente na tipificação, investigação e sanção das condutas criminosas?

Para tanto, o estudo tem como objetivo geral analisar criticamente a inter-relação entre a LGPD e o Direito Penal brasileiro, identificando as potencialidades normativas e os limites da atuação repressiva. Metodologicamente, será empregada uma revisão bibliográfica e documental, com base em literatura científica, legislações e documentos oficiais (Duarte, 2022;

Costa; Silva, 2022).

Pretende-se, assim, contribuir para o debate acadêmico e jurídico, delimitando as possibilidades de atuação da LGPD como instrumento de enfrentamento da criminalidade digital no Brasil. O artigo está estruturado em quatro seções, que abordarão, sucessivamente os fundamentos da proteção de dados e dos crimes cibernéticos, a LGPD e sua relação com o Direito Penal, os desafios na investigação e sanção dos crimes cibernéticos, e por fim, as propostas e perspectivas para a tutela penal dos dados pessoais.

2. Fundamentos da proteção de dados e dos crimes cibernéticos e a evolução da legislação no Brasil

A proteção de dados pessoais no Brasil é fruto de um processo legislativo gradual, que reflete a necessidade de acompanhar a rápida evolução tecnológica e a crescente digitalização das relações sociais.

Inicialmente, o tema era tratado de forma difusa pela Constituição Federal de 1988, que assegurava direitos à privacidade, intimidade, honra e sigilo das comunicações, mas não contemplava diretamente a proteção de dados como categoria autônoma. A ausência de uma legislação específica voltada ao ambiente digital deixava lacunas que eram supridas por normas esparsas, dificultando a efetividade na defesa da privacidade e na repressão a condutas ilícitas. Esse cenário começou a se modificar com o fortalecimento do debate sobre direitos digitais na década de 2000, impulsionado pela intensificação do uso da internet no país (Silva; Novais, 2023).

Nesse contexto, o Marco Civil da Internet (Lei nº 12.965/2014) surgiu como o primeiro grande marco regulatório brasileiro voltado à disciplina do ambiente virtual. A lei estabeleceu princípios fundamentais, como a garantia da neutralidade de rede, a proteção à privacidade e a responsabilidade dos provedores de serviços. Embora não tivesse como foco central a proteção de dados pessoais, o Marco Civil representou um avanço considerável, pois consagrou a privacidade dos usuários como direito fundamental no ambiente digital. Além disso, determinou regras para a guarda e o fornecimento de registros de conexão e acesso, criando parâmetros mínimos de segurança jurídica para a utilização da rede (Zacarias; Freire, 2023).

A partir do Marco Civil, abriu-se espaço para a discussão sobre a necessidade de uma lei específica para o tratamento de dados pessoais. Isso se intensificou diante das transformações globais no campo da proteção de dados, sobretudo após a promulgação do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), em 2016, que inspirou

diversos países a atualizarem suas legislações internas.

Nesse sentido, o Brasil, inserido em um cenário globalizado e interconectado, precisava adequar seu ordenamento jurídico para manter relações comerciais com países que já exigiam padrões mais rígidos de proteção, como os membros da União Europeia. Esse fator externo foi decisivo para acelerar a elaboração de um marco normativo nacional voltado especificamente à proteção de dados (Souza *et al.*, 2024).

Com efeito, a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) constituiu, assim, um divisor de águas. A LGPD disciplinou de forma detalhada a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais, trazendo conceitos como controlador, operador, titular de dados e bases legais para o tratamento. A lei também reforçou princípios como transparência, finalidade, necessidade e segurança, buscando equilibrar o uso econômico da informação com a preservação da dignidade humana. Sua aprovação marcou a entrada do Brasil em um novo patamar de proteção normativa, alinhando-o a padrões internacionais já consolidados (Silva; Novais, 2023).

Ademais, outro aspecto de destaque da LGPD foi a criação da Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e aplicar sanções administrativas em casos de descumprimento. Essa institucionalização foi essencial para conferir efetividade à lei, pois um dos grandes problemas das normas anteriores era a falta de órgãos especializados capazes de supervisionar o cumprimento das regras.

Com a ANPD, a legislação ganhou mecanismos concretos de *enforcement*, ainda que limitados ao campo administrativo, o que evidencia a necessidade de integração entre a tutela civil, administrativa e penal no enfrentamento de violações relacionadas a dados pessoais (Damião; Novais, 2024).

Entretanto, apesar de seus avanços, a LGPD tem como característica principal a natureza administrativa, deixando de prever tipos penais específicos para condutas relacionadas ao mau uso de dados pessoais. Essa ausência gera debates na doutrina, pois ainda que o Código Penal contemple crimes como invasão de dispositivo informático e violação de segredo, há práticas criminosas modernas, como o vazamento em massa de dados ou a comercialização ilícita de informações sensíveis, que não encontram tipificação adequada na legislação penal vigente.

Dessa forma, a LGPD contribui para a prevenção e para a responsabilização administrativa, mas revela limites quando se trata da repressão penal das condutas cibernéticas (Zacarias; Freire, 2023).

Além disso, a evolução normativa no Brasil não ocorreu de maneira linear, mas como resposta a demandas sociais e pressões internacionais. Casos emblemáticos de vazamento de

dados, fraudes eletrônicas e ataques de hackers tiveram repercussão midiática e política, pressionando o legislador a avançar na criação de normas específicas. Essa trajetória demonstra que a legislação brasileira sobre proteção de dados tem caráter reativo, mais do que preventivo, o que reforça a importância de pesquisas que analisem criticamente a efetividade das leis existentes e apontem a necessidade de aprimoramentos (Costa; Silva, 2022).

A evolução da legislação de proteção de dados no Brasil, do Marco Civil à LGPD, reflete o esforço de adaptação do ordenamento jurídico às novas dinâmicas da sociedade da informação. Contudo, esse processo está longe de ser concluído: ainda há lacunas regulatórias, desafios de aplicação e a necessidade de uma maior integração entre a LGPD e o direito penal. A revisão dessa trajetória histórica é essencial para compreender os limites atuais e os caminhos possíveis para o fortalecimento da tutela penal dos dados pessoais no país, garantindo, assim, maior segurança jurídica em um ambiente digital cada vez mais vulnerável (Duarte, 2022; Souza et al., 2024).

Portanto, percebe-se que a consolidação de um sistema jurídico eficaz de proteção de dados depende não apenas de novas leis, mas também da mudança de paradigma quanto à cultura da informação no Brasil. A legislação deve ser acompanhada de políticas públicas de conscientização, capacitação dos agentes públicos e ampliação dos mecanismos de cooperação internacional. Somente a partir dessa combinação entre normatividade, educação digital e atuação penal eficiente será possível assegurar a proteção efetiva dos direitos fundamentais dos cidadãos na era digital.

2.1 O direito à proteção de dados pessoais como direito fundamental

O reconhecimento da proteção de dados pessoais como direito fundamental representa uma conquista significativa no fortalecimento do Estado Democrático de Direito no Brasil. A Constituição Federal de 1988 já assegurava, em seu artigo 5º, a inviolabilidade da intimidade, da vida privada e do sigilo das comunicações, mas não previa a proteção de dados como categoria autônoma. Com o avanço das tecnologias digitais e a crescente circulação de informações, tornou-se evidente a necessidade de um direito específico voltado à proteção da privacidade informacional, uma vez que os dados pessoais passaram a constituir instrumentos de poder político e econômico (Silva; Novais, 2023).

Esse reconhecimento ganhou força com a Emenda Constitucional nº 115/2022, que incluiu expressamente a proteção de dados pessoais no rol dos direitos e garantias fundamentais, equiparando-a a valores como liberdade e dignidade. Segundo Souza *et al.* (2024), tal medida

“reconfigura o papel do Estado, impondo-lhe o dever de assegurar a integridade das informações pessoais como extensão da personalidade humana”. Assim, a proteção de dados deixou de ser um tema restrito à administração pública e passou a integrar a esfera dos direitos fundamentais, vinculando diretamente o Estado e a iniciativa privada ao dever de garantir segurança informacional.

A constitucionalização desse direito trouxe implicações práticas importantes, sobretudo no campo das políticas públicas e das sanções jurídicas. Como destacam Damiano e Novais (2024), que a violação de dados pessoais deve ser tratada como atentado à dignidade humana, demandando uma resposta proporcional à gravidade do dano. Essa interpretação reforça a necessidade de mecanismos jurídicos mais eficazes, inclusive penais, para lidar com condutas que utilizam a tecnologia como meio de violação de direitos.

Nesse viés, destaca-se o princípio da autodeterminação informacional, consagrado na doutrina europeia e incorporado pela LGPD, consolidando o entendimento de que cada indivíduo tem o direito de controlar o uso e a circulação de suas informações. Conforme explica Duarte (2022), o titular deve ter poder de decisão sobre seus próprios dados, o que representa uma nova dimensão da liberdade individual e da dignidade humana. No Brasil, a internalização desse princípio pela LGPD fortalece a visão de que a privacidade ultrapassa o campo patrimonial e alcança o núcleo essencial da personalidade.

Além de garantir a autonomia individual, a proteção de dados possui um caráter coletivo e social. Logo, vazamentos massivos, fraudes e ataques cibernéticos demonstram que o tratamento inadequado de informações pode comprometer não apenas a segurança de um cidadão, mas a confiança pública nas instituições. Nessa perspectiva, Costa e Silva (2022) ressaltam que a tutela penal da proteção de dados é necessária não apenas para punir condutas individuais, mas também para preservar a estabilidade das relações digitais e econômicas que sustentam a sociedade contemporânea.

No cenário internacional, a constitucionalização da proteção de dados reforça a integração do Brasil às normas globais de segurança informacional, facilitando acordos de cooperação no combate ao cibercrime. Países com legislações compatíveis tendem a colaborar de forma mais eficiente na investigação e repressão a ilícitos digitais, o que posiciona o Brasil como ator relevante nesse campo jurídico emergente (Souza *et al.*, 2024).

Apesar dos avanços, a concretização desse direito depende da efetividade de sua aplicação. O reconhecimento constitucional, por si só, não garante proteção real se não houver políticas públicas de segurança da informação, investimentos em infraestrutura tecnológica e capacitação dos órgãos de fiscalização e investigação. A falta de integração entre as esferas

administrativa, civil e penal ainda é um obstáculo à consolidação da proteção integral dos dados pessoais (Zacarias; Freire, 2023).

Dessa forma, é possível afirmar que a proteção de dados como direito fundamental não deve ser vista apenas como uma inovação legislativa, mas como um compromisso ético e político com a liberdade e a dignidade humana. O Brasil precisa avançar da formalidade normativa para a efetividade prática, promovendo uma cultura de responsabilidade digital e fortalecendo o papel do Estado e das instituições na garantia da privacidade informacional. Somente por meio dessa integração será possível consolidar uma tutela jurídica plena e adaptada à complexidade da era digital.

3. A intersecção entre a LGPD e as disposições do Código Penal Brasileiro

A intersecção entre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e o Código Penal Brasileiro configura um marco na evolução do ordenamento jurídico nacional no enfrentamento dos crimes digitais. A LGPD, embora de natureza predominantemente administrativa e civil, introduz princípios e obrigações que impactam diretamente a esfera penal, servindo de parâmetro interpretativo para a repressão de condutas que envolvem o tratamento ilícito de dados pessoais.

Nesse sentido, Silva e Novais (2023, p. 9), destacam que “a LGPD não cria tipos penais, mas orienta a aplicação do direito penal contemporâneo, especialmente em contextos de violação da privacidade informacional e do uso indevido de dados sensíveis”.

O Código Penal, por sua vez, contempla dispositivos que tangenciam a proteção da intimidade e da vida privada, como os crimes de violação de correspondência (art. 151), divulgação de segredo (art. 153) e falsidade ideológica (art. 299). Todavia, a rápida transformação digital expôs a insuficiência dessas normas tradicionais para abarcar novas formas de delinquência tecnológica. Inclusive, com a promulgação da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, representou um avanço ao tipificar a invasão de dispositivos informáticos.

Nesse ponto, convém pontuar os destaques de Zacarias e Freire (2023, p. 36), que “as normas penais brasileiras permanecem fragmentadas, carecendo de atualização sistemática para acompanhar as complexidades do ciberespaço e a sofisticação dos ataques informacionais”. Assim, a LGPD surge como instrumento complementar de política criminal preventiva, impondo às pessoas físicas e jurídicas o dever de adotar medidas de segurança técnicas e organizacionais. O descumprimento deliberado dessas obrigações pode configurar ilícitos

penais, como a violação de segredo profissional (art. 154 do Código Penal) ou o furto qualificado mediante fraude eletrônica (art. 155, §4º-B).

Dessa forma, Dias (2021, p. 46) afirma que:

As organizações precisam se adaptar à Lei Geral de Proteção de Dados, uma vez que compartilham irregularmente ou cometem vazamentos de dados, ainda que de forma accidental, estarão sujeitas a diversas penalidades, tanto da Lei supracitada quanto de outras normas vigentes. Deste modo, preliminarmente as empresas que coletam e armazenam essas informações devem implementar a LGPD, através de um fluxo de medidas contidas nela, com o intuito de evitar o compartilhamento irregular destas bases de conhecimento e rever sua política de segurança da informação, como também adequando-os, sejam eles dados pessoais sensíveis ou de crianças e adolescentes, às suas especificidades, respeitando os princípios da LGPD. Inconcebível enxergar a proteção desses conteúdos como mero ato dispendioso, ao invés de um investimento necessário e capaz de transmitir para o titular a preocupação dos agentes de tratamento para com eles, em razão de sua privacidade e segurança. Portanto, as sanções administrativas, a responsabilidade e ressarcimento de danos a partir da falta de segurança da informação e compartilhamento irregular de dados, são os instrumentos adotados pelo legislador brasileiro através do ordenamento pátrio e da LGPD, com o intuito de encorajar uma cultura de ética e baseada desde a concepção nas normas vigentes, assegurando que os prestadores de serviço estão cientes das escolhas desde a concepção que integram a privacidade e outros princípios éticos nos produtos e serviços que tratam desses elementos pessoais.

Além do aspecto material, a LGPD influencia a dimensão processual penal, estabelecendo balizas para a coleta, o armazenamento e o uso de provas digitais. O princípio da proporcionalidade, previsto implicitamente no texto da lei, exige que o tratamento de dados em investigações criminais respeite as finalidades legítimas e o direito à privacidade. Souza *et al.* (2024) enfatizam que o uso abusivo de dados sem base legal pode gerar nulidades processuais e responsabilização estatal, reforçando o papel da LGPD como instrumento de controle do poder punitivo.

Entretanto, outro ponto de convergência está na definição de dado pessoal sensível, categoria introduzida pela LGPD para delimitar informações que exigem maior proteção, como convicções religiosas, dados genéticos e biométricos. A manipulação criminosa desses dados pode agravar a pena, uma vez que o potencial de dano moral e social é significativamente mais elevado. Costa e Silva (2022) sustentam que a utilização de tais dados em práticas fraudulentas deve ser compreendida como lesão à dignidade humana, e não apenas como ofensa patrimonial.

A interface entre a Lei Geral de Proteção de Dados Pessoais e o Código Penal revela complexos desafios de ordem interpretativa e dogmática, especialmente no que concerne à necessária harmonização entre os princípios da intervenção mínima e da proporcionalidade penal e o dever estatal de assegurar uma tutela efetiva e abrangente da privacidade e da proteção dos dados pessoais. Tal conciliação demanda uma leitura sistemática que preserve a coerência do ordenamento jurídico, evitando a expansão indevida do direito penal para esferas já

suficientemente reguladas pelo direito administrativo e civil sancionador. Duarte (2022) destaca que o objetivo é evitar o “expansionismo penal” e garantir que a criminalização de condutas relacionadas ao tratamento indevido de dados ocorra apenas quando indispensável para a tutela de bens jurídicos fundamentais.

Apesar das limitações estruturais, a LGPD tem promovido avanços importantes na responsabilização de agentes que cometem ilícitos digitais. A obrigatoriedade de comunicação de incidentes de segurança, por exemplo, cria mecanismos de transparência que facilitam a atuação de órgãos como o Ministério Público e a Autoridade Nacional de Proteção de Dados (ANPD). A cooperação entre essas instituições é essencial para fortalecer a persecução penal e reduzir a impunidade nos casos de vazamento ou comercialização ilícita de informações pessoais (Silva; Novais, 2023; Souza *et al.*, 2024).

Ademais, a aplicação prática da LGPD no âmbito penal depende de uma abordagem integrada entre as instituições de justiça e a sociedade civil. É necessário que promotores, delegados e peritos digitais compreendam os fundamentos técnicos e éticos da lei, de modo a garantir a correta apuração de delitos cibernéticos. Essa interdisciplinaridade é crucial para que a legislação alcance sua finalidade social e não se restrinja à letra da norma.

Em síntese, a aproximação entre a LGPD e o Código Penal reflete o esforço do Estado brasileiro em atualizar sua política criminal diante dos desafios impostos pela era digital. Mais do que estabelecer novos tipos penais, trata-se de promover uma cultura jurídica voltada à prevenção e à responsabilização proporcional. A consolidação dessa intersecção depende de reformas legislativas que confirmem maior precisão aos crimes informacionais, mas também de uma mudança cultural, que valorize a ética no uso dos dados e a educação digital da população.

Assim, a proteção de dados pessoais deixa de ser mera diretriz administrativa e se afirmar como um verdadeiro pilar do Estado Democrático de Direito, capaz de equilibrar liberdade, segurança e responsabilidade em uma sociedade conectada.

4. Crimes cibernéticos e o papel da LGPD na prevenção e combate

A discussão sobre a necessidade de criação de novos tipos penais relacionados à proteção de dados pessoais e aos crimes cibernéticos tem ganhado crescente relevância no cenário jurídico contemporâneo. Embora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) tenha representado um avanço substancial na regulação administrativa e civil do tratamento de informações, ela não estabeleceu mecanismos penais próprios para responsabilizar condutas que causem danos graves à privacidade informacional.

Pois bem, segundo Silva e Novais, (2023), essa lacuna evidencia o desafio de adaptar o direito penal a um contexto tecnológico em constante transformação, onde novas formas de criminalidade surgem de maneira dinâmica e transnacional.

O Código Penal Brasileiro, criado em 1940, foi concebido em um contexto histórico completamente distinto, no qual as relações sociais e econômicas não dependiam de meios digitais. Apesar das reformas pontuais, como a introdução do artigo 154-A pela Lei nº 12.737/2012 (Lei Carolina Dieckmann) e da fraude eletrônica pela Lei nº 14.155/2021, o sistema penal ainda não abrange de forma suficiente a complexidade dos delitos cibernéticos. Zacarias e Freire (2023, p. 22) afirmam que:

A legislação penal brasileira, ainda que avance na criminalização da invasão de dispositivos e na proteção de sistemas informáticos, permanece aquém das demandas impostas pela sociedade da informação, deixando descobertas diversas condutas lesivas ao direito fundamental à privacidade.

De fato, as novas modalidades de ataque digital, tais como *ransomware*, *phishing* avançado, manipulação algorítmica, clonagem de identidade virtual e vazamentos massivos de dados, transcendem os limites dos tipos penais tradicionais. A LGPD, embora traga princípios e obrigações, carece de dispositivos repressivos que garantam respostas proporcionais a tais violações. Damião e Novais (2024, p. 11) ressaltam que “a ausência de tipos penais específicos que abordem a violação dolosa de dados pessoais fragiliza o sistema de proteção e compromete a efetividade das políticas públicas de segurança informacional”.

Assim, a necessidade de atualização normativa não implica um mero expansionismo penal, mas a adequação das normas punitivas à nova realidade digital. Inclusive, como bem pontuado por Almeida (2015, p. 222-223), ao afirmar que:

Proporcionalmente aos benefícios que surgiram com a internet vieram, também, condutas ilícitas praticadas por agentes especializados nesse campo. Tais comportamentos são conhecidos de diversas formas, tais como crimes virtuais, crimes cibernéticos, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, crimes de internet, fraude informática, crimes transnacionais, entre outras. Nesse âmbito, temos a figura do criminoso informático, que possui inteligência, conhecimento de sistemas de informações e usos de meios informatizados com o fim de atingir bens jurídicos alheios, fazendo-se valer de um novo universo de possibilidades de atuação criminosa. O Direito Penal encontra muitas dificuldades de adaptação dentro deste contexto.

Outrossim, a criação de figuras penais específicas voltadas à proteção de dados deve observar os princípios da intervenção mínima e da proporcionalidade. O direito penal não deve ser utilizado de forma desmedida, mas apenas quando as sanções civis e administrativas se mostram insuficientes para garantir a tutela de bens jurídicos essenciais. Nesse sentido, Costa e Silva (2022) argumentam que o tratamento ilícito de dados pessoais, quando causa danos efetivo à integridade moral ou econômica do indivíduo, deve ser enquadrado em um tipo penal próprio, com gradação de pena conforme o grau de lesividade e a intencionalidade da conduta.

A experiência internacional reforça essa necessidade, considerando que diversos países da União Europeia, em consonância com o Regulamento Geral de Proteção de Dados (GDPR), preveem sanções penais para casos graves de uso indevido de informações pessoais, sobretudo quando há dolo ou obtenção de vantagem ilícita. Essa tendência demonstra que a proteção penal dos dados é uma realidade consolidada em sistemas jurídicos maduros, nos quais a tutela da privacidade é compreendida como extensão da dignidade da pessoa humana (Duarte, 2022).

No contexto brasileiro, a proposta de novos tipos penais poderia incluir a criminalização específica do comércio ilegal de dados pessoais, da reidentificação de informações anonimizadas e do vazamento intencional de dados sensíveis. Além disso, seria necessária a atualização das penas para infrações já previstas, de modo a refletir o impacto social e econômico dessas condutas. A criação desses tipos penais permitiria maior coerência sistemática, garantindo respostas mais eficazes e compatíveis com a gravidade das ofensas cibernéticas.

A articulação entre a LGPD e o direito penal deve ocorrer de maneira complementar e harmônica. Por sua vez, a LGPD estabelece um sistema preventivo e de responsabilização administrativa, enquanto o direito penal atua como última *ratio*, assegurando a punição de condutas de maior reprovabilidade social. Essa interação deve ser guiada pelo princípio da proporcionalidade, de modo a evitar o uso excessivo da punição criminal e, ao mesmo tempo, assegurar a efetividade da proteção jurídica dos dados pessoais (Souza *et al.*, 2024).

Por fim, a criação de novos tipos penais voltados à tutela dos dados pessoais não deve ser vista como simples ampliação punitiva, mas como instrumento de atualização da política criminal frente à complexidade tecnológica contemporânea. O avanço das práticas ilícitas no ambiente digital exige um sistema penal sensível às novas formas de lesão à dignidade e à liberdade informacional, ou seja, mais do que punir, o objetivo deve ser o de promover uma cultura de segurança, transparência e responsabilidade no uso dos dados. Com isso, somente por meio dessa modernização legislativa, aliada à cooperação institucional e à educação digital, será possível consolidar uma tutela penal verdadeiramente eficaz e alinhada aos valores do Estado Democrático de Direito.

4.1 O aprimoramento dos instrumentos de investigação e coleta de provas digitais

A investigação dos crimes cibernéticos demanda instrumentos técnicos e jurídicos específicos que garantam tanto a eficácia da persecução penal quanto a observância dos direitos fundamentais. O ambiente digital introduz novos desafios probatórios, uma vez que os rastros

informáticos podem ser facilmente adulterados, apagados ou transferidos para servidores em outros países. Nesse contexto, o aprimoramento dos meios de investigação deve ocorrer em conformidade com os princípios estabelecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente os da finalidade, necessidade e proporcionalidade (Silva; Novais, 2023).

A utilização de dados pessoais em investigações criminais deve observar limites constitucionais claros. A LGPD, ao regulamentar o tratamento de informações, fornece parâmetros para evitar abusos na coleta e utilização de dados. Conforme Souza et al. (2024, p. 18), “a proteção da privacidade não se opõe à investigação criminal, mas exige que ela ocorra dentro de critérios objetivos e sob controle judicial, assegurando o equilíbrio entre segurança e liberdade”. Dessa forma, o uso de dados deve estar sempre vinculado a uma finalidade legítima e proporcional à gravidade do delito investigado.

O avanço tecnológico também exige a adoção de metodologias forenses digitais mais sofisticadas. Técnicas como a rastreabilidade de IPs, a análise de metadados e o uso de inteligência artificial em perícias devem ser incorporadas de maneira responsável e supervisionada, evitando a violação de direitos individuais. Damião e Novais (2024, p. 14) destacam que “a confiabilidade das provas digitais depende da observância rigorosa da cadeia de custódia, da integridade dos dados e da transparência dos métodos de obtenção”. Portanto, essa perspectiva reforça que a eficácia da persecução penal está diretamente relacionada à legitimidade dos meios utilizados.

Como apontado por Lima (2024, p. 34-35), veja:

A investigação criminal digital é um tema de grande relevância no contexto atual, tendo em vista o aumento da criminalidade cibernética e a necessidade de modernizar as práticas investigativas para lidar com crimes que envolvem tecnologia. [...]

No entanto, a investigação criminal digital enfrenta diversos desafios, como a volatilidade e a manipulabilidade dos dados digitais, a necessidade de protocolos rigorosos para garantir a integridade das provas e a dificuldade de rastrear alterações nos dados. [...]

Dessa forma, a proteção da privacidade e dos direitos fundamentais é um aspecto crucial no processo penal digital.

Dessarte, outro aspecto relevante é a cooperação entre os órgãos nacionais e internacionais, os crimes cibernéticos, em grande parte, ultrapassam fronteiras geográficas, exigindo a integração entre a Polícia Federal, o Ministério Público, a Autoridade Nacional de Proteção de Dados (ANPD) e organismos internacionais. Por outro lado, com a adesão do Brasil à Convenção de Budapeste sobre o cibercrime, ainda em tramitação, representaria um avanço significativo nesse sentido, ao facilitar a troca de informações e a harmonização de procedimentos.

Além disso, é imprescindível o investimento na capacitação técnica de peritos e agentes públicos. A formação interdisciplinar em direito, tecnologia e segurança da informação é fundamental para que as autoridades compreendam as peculiaridades das provas digitais e atuem com eficiência. A ausência dessa qualificação compromete a validade dos processos e favorece a impunidade.

Portanto, o aprimoramento dos instrumentos de investigação e coleta de provas digitais não se limita ao aperfeiçoamento técnico, mas envolve também o fortalecimento institucional e ético da persecução penal. É necessário construir um modelo investigativo que una eficiência e respeito aos direitos humanos, garantindo que o combate ao cibercrime ocorra sob os pilares da legalidade, da transparência e da proporcionalidade.

4.2 A importância da conscientização e do diálogo institucional para uma eficaz proteção penal de dados

A efetividade da tutela penal dos dados pessoais não depende exclusivamente da criação de normas ou do aprimoramento das ferramentas investigativas, mas também da conscientização social e do diálogo institucional entre os diversos atores do sistema de justiça. Nesse viés, a consolidação de uma cultura de proteção de dados requer a compreensão, por parte da sociedade e do Estado, de que a privacidade informacional constitui um bem jurídico essencial à dignidade humana e à cidadania digital (Costa; Silva, 2022).

Com efeito, a educação digital é um elemento fundamental nesse processo, posto que a sociedade precisa compreender os riscos associados ao compartilhamento excessivo de informações e à vulnerabilidade das plataformas tecnológicas.

Segundo Duarte (2022, p. 27), “a proteção penal dos dados só alcançará efetividade se for acompanhada de uma consciência coletiva de responsabilidade sobre o uso ético e seguro das informações pessoais”. Essa conscientização deve ser promovida por meio de políticas públicas, campanhas educativas e programas institucionais voltados tanto aos cidadãos quanto às empresas e agentes públicos.

O diálogo entre as instituições do sistema de justiça, como o Ministério Público, o Poder Judiciário, a Polícia Federal e a Autoridade Nacional de Proteção de Dados (ANPD) é outro pilar essencial para a proteção penal dos dados, considerando que a atuação integrada permite o compartilhamento de informações, a uniformização de procedimentos e a construção de estratégias conjuntas de prevenção e repressão.

Damião e Novais (2024, p. 19) enfatizam que “a proteção de dados é um desafio

transversal, que exige uma resposta coordenada entre órgãos estatais e o setor privado, sob pena de esvaziar a efetividade das sanções e comprometer a confiança social no ambiente digital”.

Nesse cenário, a Autoridade Nacional de Proteção de Dados (ANPD), em particular, tem papel estratégico na mediação entre as esferas administrativa e penal, pois sua função não é apenas fiscalizatória, mas também educativa, devendo fomentar boas práticas de governança de dados e promover o diálogo entre o Estado e a sociedade civil. Logo, a aproximação entre a ANPD e as forças de segurança pode contribuir para a detecção precoce de condutas ilícitas e para a construção de um sistema mais integrado de proteção jurídica.

Além disso, é necessário investir na formação ética e técnica dos profissionais que atuam na persecução penal, tais como os delegados, promotores, juízes e peritos precisam compreender os fundamentos da LGPD e seus reflexos no processo penal, evitando interpretações equivocadas e decisões que possam violar garantias constitucionais. Essa integração entre o conhecimento jurídico e tecnológico é indispensável para o fortalecimento de uma cultura institucional comprometida com os direitos fundamentais.

Somado a isso, nas palavras de Lopes (2023, p. 167):

A realização concreta da busca e da apreensão de elementos de prova digitais em consonância ao modelo constitucional do processo exige diversas releituras sobre a cautelaridade, os seus requisitos de admissão, o seu procedimento e a ilicitude probatória. Mormente pelo imenso potencial de vigilância possibilitado pelas novas tecnologias e a virtualização da sociedade atual, o respeito ao modelo constitucional do processo é indispensável no controle racional da atuação dos sujeitos na persecução penal.

Por fim, é importante reconhecer que a proteção penal dos dados pessoais transcende o campo jurídico e alcança dimensões políticas e sociais. O desafio não é apenas punir infratores, mas consolidar uma sociedade que valorize a privacidade, a segurança digital e o respeito à dignidade humana. O diálogo permanente entre instituições, empresas e cidadãos é o caminho para transformar a proteção de dados em um compromisso coletivo. Dessa forma, o Brasil poderá avançar na construção de um sistema penal moderno, equilibrado e humanizado, capaz de responder com eficácia e legitimidade aos desafios da era digital.

5. Considerações finais

A análise realizada ao longo deste artigo permitiu compreender que a Lei Geral de Proteção de Dados Pessoais (LGPD) constitui um marco essencial na consolidação da tutela jurídica da privacidade no Brasil, especialmente diante da crescente incidência dos crimes cibernéticos. Embora a lei tenha natureza administrativa, seus efeitos alcançam o campo penal ao estabelecer parâmetros de segurança, responsabilização e prevenção. A LGPD contribui,

assim, para estruturar um sistema normativo que busca equilibrar o desenvolvimento tecnológico com a proteção dos direitos fundamentais, reforçando a importância da autodeterminação informacional e da privacidade como pilares do Estado Democrático de Direito.

Verificou-se, contudo, que o ordenamento jurídico brasileiro ainda carece de integração normativa entre a LGPD e o Código Penal, sobretudo na tipificação de condutas específicas relacionadas ao uso ilícito de dados pessoais. Os tipos penais atualmente existentes, como invasão de dispositivo informático, estelionato virtual e violação de segredo profissional, mostram-se insuficientes para abranger as novas modalidades de crimes digitais, que evoluem de maneira acelerada e transnacional. Essa lacuna legislativa compromete a efetividade da repressão e amplia a sensação de impunidade diante de infrações que afetam milhões de cidadãos.

Além das deficiências tipológicas, persistem desafios técnicos e processuais significativos nas investigações criminais envolvendo o ciberespaço. A dificuldade de identificação dos autores, a volatilidade das provas digitais e a necessidade de cooperação internacional são obstáculos que exigem não apenas reformas legislativas, mas também investimentos em capacitação, infraestrutura e governança digital. A atuação integrada entre a Autoridade Nacional de Proteção de Dados (ANPD), o Ministério Público e as polícias especializadas é fundamental para tornar mais eficaz o combate às infrações cibernéticas.

A pesquisa também demonstrou que a efetividade da LGPD depende de uma cultura institucional de conformidade e de responsabilidade no tratamento de dados. A adoção de políticas de compliance, o uso de tecnologias de proteção e a educação digital são medidas indispensáveis para reduzir vulnerabilidades e prevenir ilícitos. Nesse sentido, a LGPD cumpre não apenas uma função regulatória, mas também pedagógica, promovendo a conscientização sobre a importância da segurança informacional tanto para o setor público quanto para o privado.

Conclui-se, portanto, que a prevenção e repressão dos crimes cibernéticos exigem uma reforma legislativa integrada, capaz de alinhar o direito penal à complexidade da sociedade digital. É necessária a criação de tipos penais específicos voltados ao tratamento indevido de dados pessoais, com penas proporcionais à gravidade das condutas e mecanismos eficazes de cooperação internacional. Além disso, recomenda-se o fortalecimento da ANPD e a ampliação das parcerias entre os órgãos de segurança e o Poder Judiciário, de modo a garantir maior eficiência na coleta e preservação de provas digitais.

Em síntese, a LGPD representa um avanço notável na proteção dos direitos fundamentais no ambiente virtual, mas sua plena efetividade depende da articulação entre prevenção, educação e repressão penal. A consolidação de um sistema penal compatível com a era da informação é indispensável para assegurar que a privacidade e a segurança de dados deixem de ser meras aspirações normativas e se tornem garantias reais e concretas, protegidas de forma eficiente pelo Estado brasileiro.

Referências

ALMEIDA, J. de J., MENDONÇA, A. B., DO CARMO, G. P., SANTOS, K. S., SILVA, L. M. M., & de AZEVEDO, R. R. D. (2015). **Crimes cibernéticos**. Caderno De Graduação - Ciências Humanas E Sociais - UNIT - SERGIPE, 2(3), 215–236. Recuperado de <https://periodicos.grupotiradentes.com/cadernohumanas/article/view/2013>

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

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Diário Oficial da União: Seção 1, Rio de Janeiro, DF, p. 23.911, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União: Seção 1, Brasília, DF, p. 1, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm.

BRASIL. **Lei nº 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: Seção 1, Brasília, DF, p. 1, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: Seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm.

COSTA, Emanuely Silva; SILVA, Raíla da Cunha. **Crimes cibernéticos e investigação policial**. Teresina: Ministério Público do Estado do Piauí, 2022. Disponível em: <https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf>. Acesso em: 3 out. 2025.

CUNHA, Vinícius Ferreira da, CORTIZO, Vitor Martins. **Crimes cibernéticos: implicações legais, eficácia das leis existentes**. Revista Acadêmica Online, [S. l.], v. 9, n. 2, 2024. Disponível em: <https://revistaacademicaonline.com/index.php/rao/article/view/122>. Acesso em: 3 out. 2025.



Ano V, v.2 2025 | submissão: 23/10/2025 | aceite: 25/11/2025 | publicação: 27/11/2025

DAMIÃO, Alisson Santana; NOVAIS, Thyara Gonçalves. **Consequências jurídicas da LGPD para os crimes virtuais**. Revista Ibero-Americana de Humanidades, Ciências e Educação – REASE, São Paulo, v. 10, n. 11, nov. 2024. Disponível em: <https://periodicorease.pro.br/rease/article/download/17054/9549/41352>. Acesso em: 3 out. 2025.

DIAS, José Lucas da Costa. **As sanções administrativas da LGPD, responsabilidade e ressarcimento de danos: uma ótica a partir da violação aos dados pessoais pelo compartilhamento irregular e falta de segurança da informação**. 2021. [56] f. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1648>. Acesso em: 07 nov. 2025.

DUARTE, Karla Lorrany da Silva. **Crimes cibernéticos e os impactos da Lei Geral de Proteção de Dados**. 2022. Monografia (Graduação em Direito) — Centro Universitário, Anápolis. Disponível em: <https://repositorio.aee.edu.br/bitstream/aee/20048/1/Karla%20Lorrany%20da%20Silva%20Duarte.pdf>. Acesso em: 3 out. 2025.

LIMA, Daniel Moura de. **A prova digital na investigação criminal**. 2024. 77 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2024.

LOPES, Marcus Vinícius Pimenta. **A participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de prova digitais**. 2023. 235 f. Tese (Doutorado em Direito) – Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2023.

MACHADO, R. L. K. **Crimes cibernéticos, invasão de privacidade e a efetividade da legislação brasileira**. Projeção e Ciência, Brasília, v. 17, n. 2, p. 45-63, 2021. Disponível em: <https://projecaociencia.com.br/index.php/Projecao2/article/view/1798>. Acesso em: 3 out. 2025.

SILVA, Ronaldo Couto da; NOVAIS, Thyara Gonçalves. **A Lei Geral de Proteção de Dados e sua aplicação no combate aos crimes cibernéticos: desafios e perspectivas**. Revista Ibero-Americana de Humanidades, Ciências e Educação – REASE, São Paulo, v. 9, n. 10, nov. 2023. DOI: 10.51891/rease.v9i10.12254. Disponível em: <https://periodicorease.pro.br/rease/article/view/12254>. Acesso em: 3 out. 2025.

SOUZA, A. P. de; SIMAS, D. C. de S.; JUSTINIANO, J. dos S.; SOUZA JUNIOR, A. M. de; LIMA, J. S. de; NORTE, N. N. B. de O.; NORTE FILHO, A. F. do; SALES, R. A. C. de; SILVA, K. A. L. da; BRITO, R. M. **Proteção digital e da defesa do consumidor no combate aos crimes cibernéticos**. Contribuciones a las Ciencias Sociales, [S. l.], v. 17, n. 10, p. e11454, 2024. DOI: 10.55905/revconv.17n.10-134. Disponível em: <https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/11454>. Acesso em: 3 out. 2025.

ZACARIAS, Fabiana; FREIRE, Lucas Zacharias. **Crimes virtuais: análise das dificuldades e desafios**. Revista JurES, Vitória, v. 16, n. 29, p. 29-61, jun. 2023. Disponível em: <https://estacio.periodicoscientificos.com.br/index.php/juresvitoria/article/download/1537/1628/2822>. Acesso em: 3 out. 2025.