

Crimes cibernéticos e a proteção das vítimas no ambiente digital

Delitos cibernéticos y la protección de las víctimas en el entorno digital

Gabriela Miranda da Silva¹

Isabela Moreira Kaule Santos²

Marisa Queiroz Castro Gomes³

Thalyta Lima Costa⁴

Luanda Patrícia dos Santos Duarte Venerio*

RESUMO: Esse artigo tem como finalidade analisar os crimes cibernéticos e os mecanismos de proteção das vítimas no ambiente digital, com enfoque na responsabilidade civil, no direito digital e na atuação do Direito Penal. Busca-se compreender de que forma o sistema jurídico brasileiro responde aos danos causados por condutas ilícitas praticadas no ciberespaço, bem como os instrumentos disponíveis para a identificação dos autores e a reparação dos prejuízos sofridos pelas vítimas. A pesquisa parte do problema relacionado à crescente incidência dos crimes virtuais e aos desafios para sua repressão e responsabilização. Utilizou-se metodologia de natureza bibliográfica e documental, baseada na análise da legislação brasileira, doutrina especializada e normas internacionais aplicáveis ao tema. Os resultados demonstram que a responsabilidade civil constitui importante mecanismo de reparação dos danos materiais e morais decorrentes destes crimes, enquanto as provas digitais e a investigação tecnológica desempenham papel fundamental na identificação dos infratores. Verificou-se ainda a relevância do Marco Civil da Internet, da Lei Geral de Proteção de Dados para o fortalecimento da segurança jurídica e da cooperação internacional. Conclui-se que a proteção das vítimas exige atuação integrada entre legislação, tecnologia e instituições responsáveis pela persecução civil e penal.

Palavras-chave: Crimes cibernéticos; Proteção das vítimas; Responsabilidade civil; Investigação digital; Direito Digital.

Abstract: Este artículo tiene como finalidad analizar los delitos cibernéticos y los mecanismos de protección de las víctimas en el entorno digital, con énfasis en la responsabilidad civil, el derecho digital y la actuación del Derecho Penal. Se busca comprender de qué manera el sistema jurídico brasileño responde a los daños causados por conductas ilícitas cometidas en el ciberespacio, así como los instrumentos disponibles para la identificación de los autores y la reparación de los perjuicios sufridos por las víctimas. La investigación parte del problema relacionado con la creciente incidencia de los delitos virtuales y los desafíos para su represión y responsabilización. Se utilizó una metodología de carácter bibliográfico y documental, basada en el análisis de la legislación brasileña, la doctrina especializada y las normas internacionales aplicables al tema. Los resultados demuestran que la responsabilidad civil constituye un importante mecanismo de reparación de los daños materiales y morales derivados de estos delitos, mientras que las pruebas digitales y la investigación tecnológica desempeñan un papel fundamental en la identificación de los infractores. Asimismo, se verificó la relevancia del Marco Civil de Internet y de la Ley General de Protección de Datos para el fortalecimiento de la seguridad

1 Faculdade de Gestão e Inovação, direito, M3, direito digital; gabriela.miranda@aluno.faculadefgi.online;

2 Faculdade de Gestão e Inovação, direito, M3; isabela@aluno.faculadefgi.online;

3 Faculdade de Gestão e Inovação, direito, M3, direito civil; marisa.gomes@aluno.faculadefgi.online;

4 Faculdade de Gestão e Inovação, direito, M3, direito penal; thalyta.costa@aluno.faculadefgi.online;

* Mestranda em Direito pelo Programa de Pós-graduação em Direito (PPGD-UFJ); Advogada da subseção de Jataí do estado de Goiás; pesquisadora de Violência Contra Mulheres; Professora na Faculdade de Gestão e Inovação (FGI), responsável pela disciplina de Metodologia da Pesquisa Científica e Produção de Textos na Turma de Direito M3; luanda.duarte@prof.faculadefgi.online

jurídica y la cooperación internacional. Se concluye que la protección de las víctimas exige una actuación integrada entre la legislación, la tecnología y las instituciones responsables de la persecución civil y penal.

Palabras-clave: Delitos cibernéticos; Protección de las víctimas; Responsabilidad civil; Investigación digital; Derecho Digital.

1. Introdução

A expansão de meios digitais e o crescente uso da internet transformaram significativamente as relações sociais, econômicas e institucionais da realidade atual. Embora esses avanços tenham proporcionado inúmeras facilidades, também propiciaram o surgimento de novas modalidades criminosas praticadas por meio de sistemas informáticos e digitais. Nesse contexto, os crimes cibernéticos passaram a representar um dos principais desafios para a segurança jurídica e para a proteção dos direitos fundamentais dos usuários do ambiente virtual, especialmente no que se refere à privacidade, à honra, à imagem e ao patrimônio das vítimas.

Os crimes cibernéticos podem ser compreendidos como condutas ilícitas praticadas por meio de dispositivos eletrônicos ou redes de comunicação digital, tendo como objetivo a obtenção de vantagens ilícitas, o acesso indevido a informações, a disseminação de conteúdos ilegais ou a prática de fraudes e extorsões. Segundo a Polícia Federal, tais delitos abrangem fraudes bancárias eletrônicas, invasões de dispositivos, disseminação de programas maliciosos, crimes de ódio e exploração sexual infantojuvenil em ambiente virtual (BRASIL, 2025).

O aumento da dependência das tecnologias digitais contribuiu para a ampliação de diversos delitos, tornando as vítimas mais vulneráveis a ataques virtuais. Conforme destacam especialistas da área, os crimes cibernéticos apresentam como uma de suas principais características a geração de rastros digitais que podem auxiliar na identificação dos autores.

Entretanto, essas evidências possuem natureza volátil, o que exige sua rápida preservação para assegurar a eficácia da investigação e a confiabilidade das provas produzidas (Rossini, 2025, p. 7)

Diante desse cenário, o ordenamento jurídico brasileiro vem desenvolvendo mecanismos normativos destinados à prevenção, repressão e responsabilização dos infratores. Destacam-se a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann⁵, o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados – LGPD (Lei nº

⁵ Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em 30 mai. 2026

13.709/2018)⁶ e, mais recentemente, o Decreto nº 12.976/2026, que estabelece diretrizes para a proteção das mulheres contra a violência digital. Esses instrumentos legislativos buscam fortalecer a proteção dos usuários e garantir maior efetividade na reparação dos danos causados pelas práticas ilícitas no ambiente virtual.

Apesar dos avanços legislativos, a crescente sofisticação das condutas criminosas e a natureza transnacional da internet ainda gera desafios à identificação dos responsáveis, à produção de provas digitais e à efetiva proteção das vítimas. Observa-se que grande parte dos estudos concentra-se na tipificação penal dos delitos cibernéticos, enquanto aspectos relacionados à proteção das vítimas, à responsabilidade civil e aos mecanismos de reparação dos danos ainda demandam maior aprofundamento acadêmico.

Nesse sentido, justifica-se a realização desta pesquisa pela relevância social e jurídica do tema, considerando o aumento expressivo dos crimes praticados no ambiente digital e seus impactos sobre indivíduos, empresas e instituições. Compreender os instrumentos legais disponíveis para a responsabilização dos infratores e para a proteção das vítimas contribui para o fortalecimento da segurança jurídica e para a efetivação dos direitos fundamentais no ciberespaço.

Dessa forma, o presente artigo tem como objetivo analisar os crimes cibernéticos e os mecanismos de proteção das vítimas no ambiente digital, com enfoque na responsabilidade civil, no direito digital e na atuação do Direito Penal, buscando compreender como o sistema jurídico brasileiro responde aos danos decorrentes dessas práticas ilícitas e quais instrumentos podem ser utilizados para a identificação dos autores e a reparação dos prejuízos sofridos pelas vítimas.

2. A responsabilidade civil nos crimes cibernéticos

Na obra de Patrícia Peck Pinheiro (2026, p. 1):

A Internet é mais que um simples meio de comunicação eletrônica, formada não apenas por uma rede mundial de computadores, mas, principalmente, por uma rede mundial de indivíduos. Indivíduos com letra maiúscula, porque estão inseridos em um conceito mais amplo, que abrange uma individualização não só de pessoas físicas, como também de empresas, instituições e governos (Pinheiro, 2026, p.1).

A partir desse entendimento, nota-se que o ambiente digital vai além da simples função de ferramenta tecnológica, que constituem em um cenário de interação social,

⁶ Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em 30 mai. 2026

econômica e institucional. Diante disso, com o crescimento da internet e das tecnologias digitais podem alterar de maneira significativa as relações sociais, dando origem a novas formas de interação, comunicação e troca de dados.

Segundo o Instituto Brasileiro de Geografia e Estatística, “ De 2023 para 2024, houve um acréscimo de 2,4 milhões de domicílios com internet” (IBGE, 2025). Nota-se no cenário atual, um aumento considerável das relações digitais, o que, consequentemente, desenvolve possibilidades de surgimento de danos no ambiente virtual. Segundo a doutrina de Nehemias Domingos de Melo podemos afirmar que:

Nos ensinamentos do Laureado Wilson Melo da Silva, os danos morais são definidos como as “lesões sofridas pelo sujeito físico ou pessoa natural de direito em seu patrimônio ideal, entendendo-se por patrimônio ideal, em contraposição ao patrimônio material. o conjunto de tudo aquilo que não seja suscetível de valor econômico”. Para melhor explicitar o seu pensar, completa o mestre: Danos morais, pois seriam, exemplificadamente, os decorrentes das ofensas à honra, ao decoro, à paz interior de cada qual, às crenças íntimas, à liberdade, à vida, à integridade corporal. (Melo, 2012, p.103).

Ainda conforme Domingos de Melo (2012) o dano moral decorre da violação de direitos ligados à personalidade e aos interesses extrapatrimoniais da pessoa, afetando elementos como a honra, imagem, privacidade, liberdade e integridade física. O autor ressalta ainda que, o dano moral pode afetar tanto pessoas físicas quanto jurídicas, especialmente quando há prejuízo à reputação, à credibilidade e ao nome. Ademais, menciona que esse tipo de dano pode surgir da lesão a valores afetivos relacionados a determinados bens materiais.

Segundo Savatier, dano moral é qualquer sofrimento que não é causado por uma perda pecuniária, para os que preferem um conceito positivo, dano moral é dor, vexame, sofrimento, desconforto, humilhação - enfim, dor da alma (Cavaliere Filho, 2026, p. 109).

Bem como os danos materiais “que constituem prejuízos ou perdas que atingem o patrimônio corpóreo de alguém” (Tartuce, 2026, p. 538), como por exemplo roubo de dados pessoais ou corporativos e seu uso para fraude financeira, espionagem ou revenda (Azam, *et al.*, 2023).

No âmbito do crime cibernético, tais ofensas decorrem uma vez que condutas degradantes infringem os direitos fundamentais. Conforme o Art. 5º inciso X da Constituição Federal “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (Brasil, 1988). Em vista disso, o Código Civil desempenha um papel crucial em seu artigo 927 que causar prejuízo a alguém, há o dever de repará-lo (Brasil, 2002).

“A responsabilidade civil surge em face do descumprimento obrigacional, pela desobediência de uma regra estabelecida em um contrato, ou por deixar determinada pessoa de observar um preceito normativo que regula a vida” (Tartuce, 2026, p. 503).

Nos termos do art. 186 do Código Civil “Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito” (Brasil, 2002). Conforme Phillips *et al* (2022) os crimes cibernéticos representam formas de atos ilícitos praticadas por meio de plataformas e softwares digitais, que podem impactar tanto pessoas, instituições quanto empresas. Entre essas práticas, destacam-se golpes virtuais, invasões de dispositivos, exposição indevida de dados pessoais e a criação de perfis falsos utilizados para disseminação de ódio e fraudes.

Segundo Cavalieri Filho (2026), a responsabilidade civil decorre da violação de um dever jurídico preexistente, impondo o agente causador do dano a obrigação de repará-lo, ressalta ainda que, embora os meios pelos quais os danos se manifestam possam evoluir, os fundamentos da responsabilidade civil permanecem os mesmos. Portanto, mesmo que no entorno digital traga novas formas, mecanismos e desafios, não há ruptura com os princípios tradicionais. Em contrapartida, reafirma-se que mesmo no domínio digital subsiste o dever jurídico fundamental de não causar danos a terceiros.

O código civil estabelece em seu art 187 que, “Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes” (Brasil, 2002).

O abuso de direito também interage com o princípio da eticidade, eis que o atual Código Civil prevê as consequências do ato ilícito para a pessoa que age em desrespeito à boa-fé, aqui prevista a boa-fé de natureza objetiva, relacionada com a conduta leal, proba e integradora das relações negociais. O art. 187 do CC/2002 consagra a função de controle exercida pela boa-fé objetiva, fazendo com que o abuso de direito esteja presente na esfera contratual, ou seja, da autonomia privada (Tartuce, 2026, p. 507)

Nesse sentido, o artigo expande a concepção do ato ilícito ao estipular que, mesmo quando um indivíduo exerce o seu direito, está sujeito a ilicitude se excede os limites estabelecidos pela boa-fé, costumes adequados e por sua finalidade social. Tal dispositivo possui relevância na conjuntura dos crimes cibernéticos, no qual ações que figuram legítimas - como liberdade de expressão, o uso de redes sociais ou a troca de informações - podem ser distorcidas para comportamentos impróprios.

A própria Constituição Federal assegura no art 5º inciso IV a livre manifestação do pensamento, vedando, contudo, o anonimato (Brasil, 1988). Ratificando que o exercício desse

direito não é absoluto e quando há violação das garantias fundamentais no ciberespaço, não impede a aplicação legal das normas jurídicas e a responsabilização civil.

Acerca da responsabilidade civil para Cavalieri Filho (2026), não surge apenas da ocorrência de um ato ilícito isolado, mas da presença conjunta de elementos essenciais, como a conduta ilícita, o dano e o nexo causal, que fundamenta o dever de reparar. Neste mesmo sentido, a conduta ilícita de acordo com Sérgio Cavalieri (2026) indica que é uma manifestação humana antijurídica, contrária ao Direito, sem qualquer referência ao elemento subjetivo ou psicológico, e também uma manifestação de vontade, uma conduta humana voluntária, só que contrária à ordem jurídica. Na internet, práticas ilegais através do uso inadequado da tecnologia, a invasão de dispositivos eletrônicos, divulgação não consentida de informações privadas, fraudes, ofensas em plataformas digitais, configuram-se ato ilícito (Santos, 2023).

Na condição dos crimes cibernéticos os efeitos ultrapassam o ambiente virtual, consequentemente produzindo consequências na esfera pessoal, social e psicológica das vítimas (Phillips *et al.*, 2022). Além da proteção constitucional, o Código Civil disciplina no art 11 que os direitos de personalidade são intransmissíveis e irrenunciáveis, reforçando a tutela jurídica da dignidade da pessoa humana (Brasil, 2002).

No art 927 do Código Civil a pessoa que, através de um ato ilícito, causar prejuízo a outro, será responsabilizado por repará-lo, e a responsabilidade existirá independentemente de culpa, nas situações previstas em lei, ou quando a atividade usualmente exercida pelo causador do dano envolver por sua natureza, risco aos direitos de outra pessoa (Brasil, 2002). Isso significa que, de acordo com Tartuce (2026 p. 521) “ todos os danos suportados pela vítima serão plenamente indenizados, sem qualquer restrição”.

Sob a perspectiva de Yuri Fisberg (2024), o dano moral é de natureza não patrimonial, por isso sua reparação não pode ser apenas considerada em termos econômicos. Nesses casos, o juiz deve analisar as circunstâncias para determinar um valor específico, que seja capaz de compensar os danos sofridos pela vítima. Dessa forma, a reparação no ambiente digital não se limita apenas ao pagamento monetário, mas também busca restaurar, na medida do possível, os direitos da personalidade violados no ambiente digital.

3. A Investigação Digital e a Proteção das Vítimas sob a Ótica da Prova

O Direito Digital pode ser compreendido como o ramo jurídico responsável por regulamentar as relações desenvolvidas no ambiente virtual, abrangendo direitos, deveres e

responsabilidades decorrentes do uso de tecnologias da informação e da internet. Com a evolução das plataformas digitais, redes sociais e sistemas de informação, foi preciso adequar o ordenamento jurídico às novas maneiras de interação social e aos crimes praticados no ambiente eletrônico.

Nesse contexto, a produção de provas digitais representa um dos principais instrumentos utilizados pelo Direito Digital no combate aos crimes cibernéticos. As provas digitais são todas as informações, em formato eletrônico, armazenadas ou transmitidas, que podem atestar a ocorrência de um ilícito no meio virtual. Mensagens, e-mails, registros de acesso, imagens, vídeos, arquivos digitais e históricos de navegação constituem exemplos de elementos frequentemente utilizados em investigações tecnológicas.

Segundo a doutrina de Guilherme Caselli podemos afirmar que: “A fonte aberta é todo o meio de busca de informações que estejam livremente dispostas...” (Caselli, 2022, p. 34) “A fonte fechada também são diferenciadas das fontes abertas por, em tese, armazenarem dados e informações classificadas como sensíveis ou pessoais.” (Caselli, 2022, p. 30)

As provas digitais podem ser obtidas tanto de fontes abertas quanto de fontes fechadas, sendo que as fontes abertas são aquelas que contêm informações acessíveis ao público na internet, e as fontes fechadas, por sua vez, armazenam dados sensíveis ou pessoais que não estão disponíveis ao público,

As provas digitais hoje são baseadas em dois pilares de dados a saber: formais e materiais. Os aspectos formais teriam relação direta com dados perfunctórios, que circundam o núcleo duro das informações.[...] Já os aspectos materiais estariam relacionados ao conteúdo das correspondências, das comunicações telegráficas, telefônicas e telemáticas. (Caselli, 2022, p. 50)

Ainda conforme Guilherme Caselli (2022) os aspectos formais estão relacionados aos dados secundários das informações, que decorrem de registros de acesso, localização, horários e identificação dos usuários, enquanto os aspectos materiais se referem diretamente ao conteúdo das comunicações, incluindo correspondências, mensagens telefônicas e telemáticas. Portanto, a produção de provas digitais abrange tanto a obtenção de informações técnicas quanto a análise do conteúdo das comunicações eletrônicas, sendo essencial para a investigação e comprovação de delitos que ocorrem no meio digital.

Além disso, o Direito Digital estabelece mecanismos legais que visam à conservação dos registros eletrônicos, especialmente através do Marco Civil da Internet. A lei nº 12.965 estabelece que à guarda de registros de conexão e acesso às aplicações de internet, permitindo

que autoridades judiciais solicitem informações necessárias para identificação dos autores de crimes cibernéticos.

A cadeia de custódia também possui grande relevância no contexto das provas digitais, assegurando que cada etapa da coleta, armazenamento e análise das evidências eletrônicas seja controlada e documentada. Dessa maneira, garante-se uma maior confiança nas informações que são empregadas durante a investigação criminal.

Portanto, percebe - se que a produção de provas digitais constitui importante instrumento do Direito Digital, permitindo que as investigações sejam efetivas, os infratores sejam responsabilizados e as vítimas do meio virtual sejam protegidas juridicamente.

A investigação de criminosos tornou - se um dos maiores desafios enfrentados pelo Direito Digital contemporâneo. O aumento das interações digitais e o avanço das tecnologias da informação têm permitido o surgimento de novos tipos de crimes cometidos pela internet, exigindo, portanto, uma atuação especializada das forças policiais e do Judiciário.

Os criminosos virtuais frequentemente utilizam mecanismos de anonimato e ferramentas tecnológicas para dificultar sua identificação, como perfis falsos, redes privadas e aplicativos criptografados. Em razão disso, a investigação digital exige métodos específicos capazes de rastrear vestígios eletrônicos deixados pelos usuários no decorrer da atividade criminosa.

A investigação digital é a utilização de métodos tecnológicos para descobrir, coletar e examinar dados eletrônicos que se relacionam a crimes cometidos na internet. Vale lembrar que os dispositivos eletrônicos, servidores, redes sociais e plataformas são responsáveis pelos delitos cibernéticos. Segundo Guilherme Caselli, “A raspagem na web é a prática de coletar dados por qualquer outro meio do que um programa interagindo com uma API”. (Caselli, 2022, p. 191) O que

Geralmente é realizado através de programa automatizado, scripts, aplicativos, extensões, bots dentre outros meios, que consultam servidores web, solicitam dados (via de regra na forma de HTML e outros arquivos que compõem páginas da web) e analisam esses dados para extrair em formação. (Caselli, 2022, p. 191)

A partir desse entendimento, é possível afirmar que a raspagem de dados possui um papel fundamental no combate aos crimes cibernéticos, uma vez que possibilita a coleta e a análise de informações importantes disponíveis no ambiente virtual, tornando-se um recurso valioso na investigação digital e na identificação de evidências relacionadas a delitos cometidos no ambiente eletrônico.

Nesse contexto, o direito digital possui papel essencial na regulamentação das investigações que ocorrem no ambiente virtual, garantindo um equilíbrio entre a segurança pública e os direitos fundamentais dos cidadãos. Dessa forma, a obtenção de registros eletrônicos, por exemplo, só pode ocorrer com autorização judicial e deve observar as garantias constitucionais da privacidade e da intimidade do usuário.

A perícia digital também representa importante mecanismo de investigação, possibilitando a análise de arquivos, históricos de navegação, registros de IP, mensagens e outros dados armazenados em dispositivos eletrônicos. Essas informações auxiliam na reconstrução dos fatos e na comprovação da autoria dos delitos virtuais.

Além disso, vários crimes cibernéticos têm uma natureza transnacional, com servidores situados em diferentes nações. Logo, o direito digital também necessita de uma cooperação internacional entre as autoridades policiais e judiciais para que se possa combater de forma mais eficiente as práticas delituosas que acontecem na internet.

Portanto, percebe - se que a investigação de criminosos virtuais exige constante atualização tecnológica, a aplicação das normas de direito digital e a colaboração entre várias instituições para reduzir a impunidade e garantir uma segurança jurídica maior no meio digital.

A investigação digital possui papel essencial na proteção das vítimas de crimes cibernéticos, principalmente com o aumento das ações ilegais que ocorrem no ambiente virtual. O direito digital tem como objetivo fornecer meios legais que protejam os usuários da internet e punam adequadamente os autores de crimes.

Entre os principais crimes cibernéticos destacam - se fraudes eletrônicas, invasão de dispositivos, vazamento de dados pessoais, cyberbullying, perseguição virtual e divulgação de imagens íntimas sem autorização. Essas condutas muitas vezes resultam em prejuízos psicológicos, morais e financeiros para as vítimas, atingindo diretamente sua dignidade e integridade pessoal.

Conforme Guilherme Caselli (2022), a investigação digital depende da correta preservação e análise das evidências eletrônicas, uma vez que os registros digitais armazenados em dispositivos, redes e plataformas virtuais podem auxiliar diretamente na identificação dos autores dos delitos cibernéticos. Nesse contexto, a preservação das provas digitais torna - se fundamental para garantir maior efetividade às investigações e possibilitar adoção de medidas judiciais voltadas à proteção das vítimas.

A Constituição Federal assegura em seu artigo 5º , inciso X, que: “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à

indenização pelo dano material ou moral decorrente de sua violação”. Dessa forma, os direitos fundamentais permanecem protegidos mesmo no ambiente virtual.

Além da responsabilização penal dos infratores, o direito digital também assegura o direito à reparação civil pelos danos causados às vítimas. O Código Civil prevê que quem causar dano a outrem tem obrigação de indenizar, inclusive no que diz respeito a atos ilícitos praticados por meio digital.

Assim, a investigação tecnológica torna - se mecanismos indispensáveis para garantia de proteção jurídica às vítimas dos crimes cibernéticos.

A proteção de dados pessoais tornou - se um dos temas centrais do direito digital contemporâneo, especialmente considerando o aumento da circulação de informações na internet. O avanço tecnológico acelerou a coleta, o armazenamento e o compartilhamento de dados pessoais por empresas, plataformas digitais e usuários da internet.

Os crimes cibernéticos frequentemente envolvem a utilização indevida de informações restritas, como documentos pessoais, senhas, dados bancários e outros registros sigilosos. Essas informações podem ser utilizadas para aplicações de golpes financeiros, extorsões, fraudes eletrônicas e outros delitos praticados no ambiente virtual.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) representa importante mecanismo jurídico destinado à proteção da privacidade e da segurança das informações pessoais. A legislação estabelece regras relacionadas ao tratamento de dados, impondo responsabilidades às instituições que realizam coleta e armazenamento dessas informações.

Conforme Guilherme Caselli (2022), a investigação digital depende diretamente da preservação e análise adequada das informações eletrônicas, uma vez que dispositivos, sistemas e plataformas digitais armazenam evidências relevantes para identificação de práticas criminosas no ambiente virtual. O autor também demonstra que os registros digitais e os mecanismos tecnológicos de segurança possuem grande importância para prevenção de acessos indevidos e proteção das informações pessoais.

Além disso, a Constituição Federal de 1988 assegura a proteção da intimidade, vida privada e imagem das pessoas, garantindo reparação em casos de violação desses direitos fundamentais. Dessa forma, percebe - se que a proteção de dados pessoais constitui importante instrumento do direito digital, pois fortalece a segurança da informação, previne crimes cibernéticos e oferece uma proteção legal aos usuários no ambiente digital.

Portanto, percebe - se que a proteção de dados pessoais constitui importante instrumento do direito digital, promovendo a segurança da informação, a prevenção de crimes virtuais e a proteção das vítimas no meio digital.

4. Direito Penal e segurança no meio digital

O avanço das Tecnologias da Informação e Comunicação (TICs) transformou a estrutura social contemporânea. Por um lado, a transição para a era digital otimizou processos, aproximou indivíduos e democratizou o acesso à informação, por outro, acabou favorecendo para o surgimento de novas condutas criminosas. Delitos como a invasão de dispositivos informáticos, golpes financeiros virtuais, extorsões, vazamento de dados pessoais e ataques cibernéticos em larga escala tornaram-se cotidianos. Esse panorama impõe ao Direito Penal e aos órgãos de segurança pública o urgente desafio de formular respostas céleres e eficazes, capazes de tutelar de forma eficiente os bens jurídicos dos cidadãos no ambiente virtual.

Historicamente, o desenvolvimento científico e tecnológico atua como o principal pilar de transformação. Desde a eclosão da Primeira Revolução Industrial, no final do século XVIII na Inglaterra, a humanidade experimenta um processo contínuo de inovação que controla o ritmo da vida em sociedade. Todavia, foi nas últimas décadas, com o advento da internet, que essa evolução adquiriu um aumento expressivo e sem precedentes. Essa mudança acelerada reconfigurou as esferas política, econômica e social em escala global.

Essa nova configuração civilizatória é classificada pela doutrina sociológica, notadamente por Manuel Castells, como a "Era da Informação", que dá origem à chamada "Sociedade Informacional". Esse é um modelo cultural e socioeconômico em que a informação e o conhecimento deixam de ser meros acessórios e passam a desempenhar um papel estratégico central. Existe uma fusão indissociável entre o plano real e o cibernético, alterando radicalmente a percepção de tempo e espaço.

Como reflexo dessa migração social para o ciberespaço, a criminalidade também se modernizou, assumindo contornos de massa. Diante da insuficiência dos métodos tradicionais de policiamento para lidar com o crime virtual, o Estado foi forçado a modernizar seus mecanismos de controle social e persecução penal. É nesse cenário que a Investigação Criminal Tecnológica assume um papel relevante para a garantia da segurança pública.

A Investigação Criminal Tecnológica é definida como o conjunto especializado de procedimentos, metodologias e recursos técnicos voltados ao levantamento de dados e análise de evidências digitais. Essa modalidade investigativa se vale de ferramentas de inteligência cibernética, softwares de processamento de grandes volumes de dados (Big Data), técnicas de extração de dados em dispositivos apreendidos, análise de fontes abertas e interceptações de

fluxos telemáticos. Longe de se restringir aos crimes puramente virtuais, o emprego dessas tecnologias é indispensável para a elucidação de crimes, cujo os atos, de execução ou ocultação deixam rastros no ambiente digital.

No plano legislativo, o ordenamento buscou acompanhar essa transição de forma gradativa. Um marco inicial relevante foi a Lei nº 12.735/2012, que em seu artigo 4º determinou expressamente que os órgãos de polícia judiciária organizassem setores e equipes especializadas para o combate a crimes praticados em redes de computadores ou sistemas informatizados. Posteriormente, a promulgação da Lei nº 12.965/2014, conhecida como o Marco Civil da Internet, trouxe a necessária segurança jurídica ao regular os parâmetros de obtenção de provas digitais, servindo como alicerce para o Poder Judiciário e evitando decisões conflitantes sobre a matéria.

O Marco Civil da Internet estabeleceu regras claras de cooperação ao prever a possibilidade de fornecimento dos registros de conexão e de acesso a aplicações. Para garantir a rapidez das investigações, permitiu-se que dados cadastrais (como qualificação pessoal, filiação e endereço) sejam requisitados diretamente pelas autoridades policiais e pelo Ministério Público aos provedores, sem a necessidade de intervenção judicial prévia. Contudo, o acesso ao conteúdo das comunicações e aos registros de navegação permanece estritamente condicionado à prévia autorização do Poder Judiciário.

Apesar dos avanços normativos, a eficácia da persecução penal enfrenta severos obstáculos de ordem técnica no dia a dia policial. A identificação do endereço de IP (Internet Protocol), embora essencial para apontar a origem de um acesso, não se traduz automaticamente na identificação imediata da autoria delitiva. É comum que um único endereço IP seja compartilhado simultaneamente por dezenas ou centenas de usuários através de tecnologias de transição de protocolos, como o Carrier-Grade NAT (CGNAT), em redes domésticas, corporativas ou condominiais. Práticas operacionais demonstram casos alarmantes em que um único IP esteve vinculado a mais de mil dispositivos ao mesmo tempo, dificultando a individualização da conduta e exigindo um aprofundamento investigativo minucioso antes de se pleitear medidas cautelares, como a busca e apreensão ou prisões temporárias e preventivas.

Soma-se a essa barreira técnica a resistência de determinados provedores de conexão e aplicação em atualizar seus sistemas ou cooperar com o Estado. A demora no fornecimento de dados e o compartilhamento excessivo de IPs geram lacunas de impunidade, prejudicando a identificação de autores de crimes graves, que vão desde fraudes financeiros complexas e crimes eleitorais até a difusão de material de abuso e exploração sexual infantil.

Reconhecendo o caráter transfronteiriço do cibercrime, o Brasil deu um passo crucial rumo à cooperação internacional ao ratificar a Convenção de Budapeste sobre Cibercriminalidade (CETS 185). O tratado, originado no Conselho da Europa e vigente internacionalmente desde 2004, teve sua adesão concluída pelo Brasil e foi promulgado internamente pelo Decreto nº 11.491/2023, passando a vigorar plenamente no território nacional.

A Convenção de Budapeste funciona como um poderoso instrumento vinculante que visa harmonizar as legislações penais e processuais penais dos países signatários. O tratado tipifica de forma padronizada condutas contra dados e sistemas informáticos, falsificações e fraudes eletrônicas, além de crimes de conteúdo, como a pornografia infantil e a violação de direitos autorais. O maior ganho prático para o cenário nacional reside no aperfeiçoamento dos mecanismos de assistência mútua, permitindo que as autoridades brasileiras solicitem a preservação rápida de dados e a obtenção de provas digitais armazenadas no exterior com uma agilidade que os canais diplomáticos tradicionais não comportavam.

O principal objetivo da intervenção do Direito Penal no ambiente virtual deve ser a proteção integral da vítima e a redução de sua vulnerabilidade digital. No ciberespaço, a vítima de um crime encontra-se frequentemente em uma posição de grande desvantagem: sua intimidade pode ser violada instantaneamente, seus ativos financeiros podem ser dissipados em segundos e sua identidade pode ser usurpada com facilidade. A Investigação Criminal Tecnológica, portanto, não serve apenas como uma ferramenta de punição do infrator, mas como um meio estatal capaz de fazer cessar a lesão jurídica e restaurar a segurança do cidadão.

Por essa razão, o Marco Civil da Internet é frequentemente descrito como "Constituição da Internet", pois ao mesmo tempo em que fornece instrumentos para a repressão de delitos, blinda os direitos fundamentais do usuário comum. O texto legal ratifica expressamente as garantias constitucionais da privacidade, da intimidade e do sigilo das comunicações de dados.

O ordenamento jurídico brasileiro adota uma postura de equilíbrio: o dever estatal de investigar e proteger a coletividade não pode atropelar as liberdades individuais. Consequentemente, qualquer prova digital obtida sem o cumprimento das exigências legais ou em desrespeito ao direito à privacidade, sem a devida justificativa e autorização judicial, será considerada inválida e não poderá ser utilizada no processo penal.

Por fim, no que tange à responsabilização, o debate penal contemporâneo deve se concentrar também na conduta das pessoas jurídicas que operam as plataformas e provedores

de internet. Embora a legislação brasileira admite a responsabilização penal da pessoa jurídica apenas em situações específicas, o descumprimento intencional de ordens judiciais de interceptação de comunicações ou de quebra de sigilo por grandes empresas de tecnologia deve receber uma resposta firme do Estado.

Para além da discussão acerca da aplicação de penas privativas de liberdade, o ordenamento jurídico dispõe de sanções alternativas eficazes para constranger as empresas de tecnologia a cooperarem com a justiça na proteção das vítimas. O próprio Marco Civil da Internet prevê, em seu artigo 12, uma gradação de sanções administrativas e coercitivas aplicáveis às empresas que violarem o sigilo ou descumprirem as ordens de preservação de dados. Essas sanções incluem: Multas pecuniárias expressivas, calculadas com base no faturamento do grupo econômico no Brasil; Suspensão temporária das atividades de coleta, armazenamento e tratamento de dados; Proibição total de exercer suas atividades em território nacional, inviabilizando a operação da empresa no país.

Dessa forma, o fortalecimento da segurança digital não depende apenas da criação de novos tipos penais, mas sim da articulação coordenada entre uma polícia judiciária tecnologicamente capacitada, uma legislação que respeite as garantias fundamentais e a aplicação de medidas coercitivas severas sobre as empresas privadas de tecnologia. Somente através desse tripé será possível garantir um ambiente virtual seguro, onde os direitos das vítimas sejam efetivamente resguardados e a impunidade dos crimes cibernéticos seja combatida com eficácia.

5. Considerações finais

Diante do que foi exposto neste artigo, mostra-se que os crimes cibernéticos representam um dos maiores desafios contemporâneos no âmbito jurídico, especialmente em razão da rápida evolução das tecnologias digitais e da ampliação das formas de interação no ambiente virtual. A expansão do uso da internet, embora tenha proporcionado benefícios, também contribuiu significativamente para o surgimento de novas modalidades de delitos, exigindo constante adaptação do Direito para lidar com os crimes e sua responsabilização.

Nota-se que o ordenamento jurídico brasileiro dispõe de diversos instrumentos normativos voltados à prevenção, repressão e responsabilização das condutas ilícitas praticadas no ambiente digital, com destaque para o Marco Civil da Internet, a Lei Geral de Proteção de Dados e demais dispositivos legais que reforçam a tutela dos direitos

fundamentais. Esses mecanismos demonstram o esforço legislativo em garantir maior segurança jurídica e efetividade na proteção dos usuários.

No que se refere à responsabilidade civil, é notório sua relevância como instrumento **para** a reparação dos danos materiais e morais sofridos pelas vítimas de crimes cibernéticos. Ainda que o ambiente digital apresenta particularidades, os fundamentos clássicos da responsabilidade civil permanecem aplicáveis, assegurando o dever de indenizar sempre que presentes os elementos do ato ilícito, do dano e do nexo causal.

Além disso, existe uma grande importância da investigação digital e da produção de provas eletrônicas como elementos fundamentais para a identificação dos autores e para a efetivação da justiça. Entretanto, a instabilidade das evidências digitais e a complexidade técnica das investigações impõem inúmeros desafios às autoridades, exigindo constante atualização tecnológica e cooperação entre instituições nacionais e internacionais.

Por fim, conclui-se que a proteção das vítimas de crimes cibernéticos depende de uma atuação integrada entre legislação, tecnologia e sistema de justiça, de modo a garantir não apenas a responsabilização dos infratores, mas também a efetiva reparação dos danos e a preservação dos direitos fundamentais no ambiente virtual. Dessa forma, torna-se indispensável o fortalecimento contínuo das políticas de segurança digital e da conscientização dos usuários da internet.

Referências

AZAM, H. et al. Cybercrime Unmasked: Investigating Cases and Digital Evidence. *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence*, v. 2, n. 1, 25 nov. 2023. Disponível em: <https://ojs.ijemd.com/index.php/ComputerScienceAI/article/view/25525>. Acesso em: 06 mai. 2026.

BRASIL. *Constituição da República Federativa do Brasil, de 5 de outubro de 1988*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 03 mai. 2026.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm. Acesso em: 04 mai. 2026.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 mai. 2026.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 31 mai. 2026.

BRASIL. *Decreto nº 12.976, de 20 de maio de 2026*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12976.htm. Acesso em: 31 mai. 2026.

BRASIL. *Superior Tribunal de Justiça*. RMS 046685 (decisão monocrática). Ministro Leopoldo de Arruda Raposo (Desembargador convocado do TJ/PE). DJE, 06 abr. 2015. Disponível em: <http://www.stj.jus.br/SCON/decisoes/doc.jsp?livre=mlat+e+google&b=DTXT&p=true&t=JURIDICO&l=10&i=1>. Acesso em: 31 mai. 2026.

BRASIL. *Ministério Público Federal*. Roteiro de Atuação sobre Crimes Cibernéticos. Brasília: MPF, out. 2013.

CASSELLI, Guilherme. *Manual de investigação criminal*. Rio de Janeiro: Juspodivm, 2022.

FISBERG, Yuri. *Dano social: reparação, aspectos processuais e destinação*. São Paulo: Almedina Brasil, 2024.

FILHO, Sérgio C. *Programa de responsabilidade civil*. 17. ed. Rio de Janeiro: Atlas, 2026.

IBGE. Acesso à internet cresce e chega a 93,6% dos domicílios do País em 2024. Disponível em: <https://agenciagov.ebc.com.br/noticias/202507/internet-chega-a-74-9-milhoes-de-domicilios-do-pais-em-2024>. Acesso em: 02 mai. 2026.

JORGE, Higor Vinicius Nogueira. (Coord.). *Tratado de Investigação Criminal Tecnológica*. Rio de Janeiro: Juspodivm, 2020.

JUSBRAZIL. *O que são crimes cibernéticos*. Disponível em: <https://www.jusbrasil.com.br/artigos/o-que-sao-crimes-ciberneticos/1583984125>. Acesso em: 31 mai. 2026.

MELO, Nehemias Domingos de. *Dano moral nas relações de consumo: doutrina e jurisprudência*. 2. ed. Rio de Janeiro: Saraiva Jur, 2012.

MINISTÉRIO PÚBLICO FEDERAL. *Roteiro de atuação sobre crimes cibernéticos*. Brasília: MPF, 2013.

NIGRI, Deborah Fisch. *Crimes e segurança na Internet*. In Verbis, Rio de Janeiro: Instituto dos Magistrados do Brasil, ano 4, n. 20, 2000.

PINHEIRO, Patrícia P. *Direito digital*. 8. ed. Rio de Janeiro: SRV, 2026. E-book. ISBN 9786553624979.

PHILLIPS, K. et al. *Conceptualizing cybercrime: definitions, typologies and taxonomies*. Forensic Sciences, v. 2, n. 2, p. 379–398, 16 abr. 2022. Disponível em: <https://www.mdpi.com/2673-6756/2/2/28>. Acesso em: 06 mai. 2026.

TARTUCE, Flávio. *Manual de direito civil: volume único*. 16. ed. Rio de Janeiro: Método, 2026.

UNIVERSIDADE FEDERAL DO PARANÁ (UFPR). *Investigação de crimes cibernéticos e governança: texto complementar aula 1*. Disponível em:

https://escola.mpu.mp.br/plataforma-aprender/acervo-educacional/conteudo/201cinvestigacao-de-crimes-ciberneticos/texto-complementar-aula-1_crimes-ciberneticos-e-governanca_revisao-final-pano-para-manga_180621.pdf. Acesso em: 31 mai. 2026.