

**II ENCONTRO NACIONAL DE
DIREITO DO FUTURO - II ENDIF**

DIREITO PENAL E TECNOLOGIA I

D598

Direito penal e tecnologia I [Recurso eletrônico on-line] organização II Encontro Nacional de Direito do Futuro: Escola Superior Dom Helder Câmara – Belo Horizonte;

Coordenadores: Camila Martins de Oliveira e Gabriela Emanuele de Resende – Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC, 2025.

Inclui bibliografia

ISBN: 978-65-5274-383-1

Modo de acesso: www.conpedi.org.br em publicações

Tema: Justiça social e tecnológica em tempos de incerteza.

1. Direito do Futuro. 2. Justiça Social. 3. Justiça Tecnológica. I. II Encontro Nacional de Direito do Futuro (1:2025 : Belo Horizonte, MG).

CDU: 34

II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

DIREITO PENAL E TECNOLOGIA I

Apresentação

O II Encontro Nacional de Direito do Futuro (II ENDIF), organizado pelo Centro Universitário Dom Helder com apoio técnico do Conselho Nacional de Pesquisa e Pós-graduação em Direito – CONPEDI, reafirma-se como um espaço qualificado de produção, diálogo e circulação do conhecimento jurídico, reunindo a comunidade científica em torno de um propósito comum: pensar, com rigor metodológico e sensibilidade social, os caminhos do Direito diante das transformações que marcam o nosso tempo. Realizado nos dias 09 e 10 de outubro de 2025, em formato integralmente on-line, o evento assumiu como tema geral “Justiça social e tecnológica em tempos de incerteza”, convidando pesquisadoras e pesquisadores a enfrentar criticamente os impactos da inovação tecnológica, das novas dinâmicas sociais e das incertezas globais sobre as instituições jurídicas e os direitos fundamentais.

Nesta segunda edição, os números evidenciam a força do projeto acadêmico: 408 trabalhos submetidos, com a participação de 551 pesquisadoras e pesquisadores, provenientes de 21 Estados da Federação, culminando na organização de 31 e-books, que ora se apresentam à comunidade científica. Essa coletânea traduz, em linguagem acadêmica e compromisso público, a vitalidade de uma pesquisa jurídica que não se limita a descrever problemas, mas busca compreendê-los, explicar suas causas e projetar soluções coerentes com a Constituição, com os direitos humanos e com os desafios contemporâneos.

A publicação dos 31 e-books materializa um processo coletivo que articula pluralidade temática, densidade teórica e seriedade científica. Os textos que compõem a coletânea passaram por avaliação acadêmica orientada por critérios de qualidade e imparcialidade, com destaque para o método double blind peer review, que viabiliza a análise inominada dos trabalhos e exige o exame por, no mínimo, dois avaliadores, reduzindo subjetividades e preferências ideológicas. Essa opção metodológica é, ao mesmo tempo, um gesto de respeito à ciência e uma afirmação de que a pesquisa jurídica deve ser construída com transparência, responsabilidade e abertura ao escrutínio crítico.

O II ENDIF também se insere em uma trajetória institucional já consolidada: a primeira edição, realizada em junho de 2024, reuniu centenas de pesquisadoras e pesquisadores e resultou na publicação de uma coletânea expressiva, demonstrando que o Encontro se consolidou, desde o início, como um dos maiores eventos científicos jurídicos do país. A

continuidade do projeto, agora ampliada em escopo e capilaridade, reafirma a importância de se fortalecer ambientes acadêmicos capazes de integrar graduação e pós-graduação, formar novas gerações de pesquisadoras e pesquisadores e promover uma cultura jurídica comprometida com a realidade social.

A programação científica do evento, organizada em painéis temáticos pela manhã e Grupos de Trabalho no período da tarde, foi concebida para equilibrar reflexão teórica, debate público e socialização de pesquisas. Nos painéis, temas como inteligência artificial e direitos fundamentais, proteção ambiental no sistema interamericano, proteção de dados e herança digital foram tratados por especialistas convidados, em debates que ampliam repertórios e conectam a produção acadêmica aos dilemas concretos vividos pela sociedade.

A programação científica do II ENDIF foi estruturada em dois dias, 09 e 10 de outubro de 2025, combinando, no período da manhã, painéis temáticos com exposições de especialistas e debates, e, no período da tarde, sessões dos Grupos de Trabalho. No dia 09/10 (quinta-feira), após a abertura, às 09h, realizou-se o Painel I, dedicado aos desafios da atuação processual diante da inteligência artificial (“Inteligencia artificial y desafios de derechos fundamentales en el marco de la actuación procesal”), com exposição de Andrea Alarcón Peña (Colômbia) e debate conduzido por Caio Augusto Souza Lara. Em seguida, às 11h, ocorreu o Painel II, voltado à proteção ambiental no Sistema Interamericano, abordando a evolução da OC-23 ao novo marco da OC-32, com participação de Soledad Garcia Munoz (Espanha) e Valter Moura do Carmo como palestrantes, sob coordenação de Ricardo Stanziola Vieira. No período da tarde, das 14h às 17h, desenvolveram-se as atividades dos Grupos de Trabalho, em ambiente virtual, com apresentação e discussão das pesquisas aprovadas.

No dia 10/10 (sexta-feira), a programação manteve a organização: às 09h, foi realizado o Painel III, sobre LGPD e a importância da proteção de dados na sociedade de vigilância, com exposições de Laís Furuya e Júlia Mesquita e debate conduzido por Yuri Nathan da Costa Lannes; às 11h, ocorreu o Painel IV, dedicado ao tema da herança digital e à figura do inventariante digital, com apresentação de Felipe Assis Nakamoto e debate sob responsabilidade de Tais Mallmann Ramos. Encerrando o evento, novamente no turno da tarde, das 14h às 17h, seguiram-se as sessões dos Grupos de Trabalho on-line, consolidando o espaço de socialização, crítica acadêmica e amadurecimento das investigações apresentadas.

Ao tornar públicos estes 31 e-books, o II ENDIF reafirma uma convicção essencial: não há futuro democrático para o Direito sem pesquisa científica, sem debate qualificado e sem compromisso com a verdade metodológica. Em tempos de incerteza — tecnológica, social,

ambiental e institucional —, a pesquisa jurídica cumpre um papel civilizatório: ilumina problemas invisibilizados, questiona estruturas naturalizadas, qualifica políticas públicas, tensiona o poder com argumentos e oferece horizontes normativos mais justos.

Registramos, por fim, nosso reconhecimento a todas e todos que tornaram possível esta obra coletiva — autores, avaliadores, coordenadores de Grupos de Trabalho, debatedores e equipe organizadora —, bem como às instituições e redes acadêmicas que fortalecem o ecossistema da pesquisa em Direito. Que a leitura desta coletânea seja, ao mesmo tempo, um encontro com o que há de mais vivo na produção científica contemporânea e um convite a seguir construindo, com coragem intelectual e responsabilidade pública, um Direito à altura do nosso tempo.

Belo Horizonte-MG, 16 de dezembro de 2025.

Prof. Dr. Paulo Umberto Stumpf – Reitor do Centro Universitário Dom Helder

Prof. Dr. Franclim Jorge Sobral de Brito – Vice-Reitor e Pró-Reitor de Graduação do Centro Universitário Dom Helder

Prof. Dr. Caio Augusto Souza Lara – Pró-Reitor de Pesquisa do Centro Universitário Dom Helder

DIREITO À PRIVACIDADE E CRIMES DIGITAIS: A RELATIVIZAÇÃO DE GARANTIAS EM PROL DA INVESTIGAÇÃO

RIGHT TO PRIVACY AND CYBERCRIMES: BALANCING FUNDAMENTAL RIGHTS AND CRIMINAL INVESTIGATION

**Caio Vinícius Soares da Silva
Victor Gustavo Rocha Nylander
Rayllana Silva Peixoto**

Resumo

O trabalho examina a relação entre o direito à privacidade digital e a investigação de crimes virtuais. Partindo da Convenção 108 do Conselho da Europa, da Constituição Federal de 1988, da LGPD e do Marco Civil da Internet, analisa-se como a proteção de dados pode ser relativizada em prol da persecução penal. Destaca-se que, embora a tutela da intimidade seja essencial, ela não pode servir como barreira absoluta contra a responsabilização de ilícitos digitais. Conclui-se que é necessário equilíbrio entre a preservação de garantias individuais e a efetividade das investigações criminais.

Palavras-chave: Privacidade digital, Proteção de dados, Crimes virtuais, Investigação criminal, Direitos fundamentais

Abstract/Resumen/Résumé

This study examines the relationship between the right to digital privacy and the investigation of cybercrimes. Based on the Council of Europe's Convention 108, the Brazilian Federal Constitution of 1988, the General Data Protection Law, and the Civil Rights Framework for the Internet, it analyzes how data protection may be relativized in favor of criminal prosecution. While the protection of privacy is essential, it cannot serve as an absolute barrier against accountability for digital crimes. The study concludes that balance is required between safeguarding individual rights and ensuring the effectiveness of criminal investigations.

Keywords/Palabras-claves/Mots-clés: Digital privacy, Data protection, Cybercrimes, Criminal investigation, Fundamental rights

1. Direito e privacidade digital

É notório o quanto a tecnologia se faz presente no cotidiano do corpo social atual, seja na forma de comunicação, entretenimento, pesquisa ou mesmo na prática de crimes. Nessa perspectiva, tornam-se necessários mecanismos capazes de ordenar os espaços virtuais.

Na década de 1970, surgiram as primeiras leis com intuito de garantir segurança digital, voltadas especificamente à proteção de dados, como a Lei de Hesse, na Alemanha (1970). Não demorou até que, em 1981, fosse firmado o primeiro acordo internacional juridicamente vinculante à defesa da intimidade digital: a Convenção 108 do Conselho da Europa. Assim, tópicos essenciais foram discutidos, muitos dos quais permanecem relevantes até os dias de hoje.

A título exemplificativo, tem-se o artigo 11º do referido tratado, em sua versão modernizada de 2018, que apresenta as restrições que atingem a tutela da privacidade informacional já estabelecida pela própria convenção. Este dispositivo legal enfatiza a possibilidade de que direitos e obrigações relativos à preservação da vida privada no meio virtual sofram restrições, caso se revele necessário em uma sociedade democrática. Nesse sentido, vale ressaltar uma dessas moderações: a limitação em casos de investigação criminal e de proteção da segurança pública.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) prevê, em seu artigo 7º, analogamente ao tratado internacional de 1981, que em hipóteses específicas — como, por exemplo, em obrigações legais — é autorizado o tratamento de dados pessoais do indivíduo.

Sob essa ótica, é possível ilustrar a problemática com uma situação hipotética: um aplicativo que armazena diversos servidores online, conectando pessoas por meio de canais de texto e voz, protegido por leis de proteção de dados e pela política de privacidade da empresa. Todavia, criminosos podem se aproveitar dessa estrutura para coagir jovens, utilizando-se de abordagens padronizadas em redes sociais. Após conquistar a confiança das vítimas, especialmente adolescentes em situação de vulnerabilidade psicológica, esses criminosos obtêm imagens íntimas de cunho sexual e, por meio de chantagem, submetem-nas a desafios desumanos, como a automutilação, exigindo ainda o compartilhamento desse material nos servidores.

Nesse contexto, os autores poderiam responder por crimes como coação (art. 146, CP), constrangimento ilegal com fim libidinoso (arts. 213 e 215, CP), além de induzimento ao

suicídio ou à automutilação (art. 122, CP, alterado pela Lei nº 13.968/2019), entre outros. Contudo, essas acusações só poderiam ser efetivamente instauradas se os órgãos competentes tomassem conhecimento do ocorrido, o que, muitas vezes, não acontece. Essa impunidade parcial é legitimada por normas brasileiras, como o art. 5º, XII, da Constituição Federal de 1988, que garante a inviolabilidade das comunicações e dados, permitindo sua quebra apenas mediante ordem judicial.

Embora o objetivo desses dispositivos seja proteger a integridade dos cidadãos, eles por vezes dificultam o acesso rápido das autoridades a elementos cruciais para investigações, especialmente em casos de plataformas estrangeiras, em que a cooperação jurídica internacional é indispensável. Portanto, evidencia-se que a mesma estrutura normativa que garante os direitos de privacidade virtual também influencia diretamente na carência de agilidade ou até mesmo na inviabilização da persecução penal em crimes digitais.

2. O processo de investigação no âmbito digital

É imprescindível compreender o funcionamento de uma investigação na esfera digital para uma melhor assimilação do tema em análise. No Brasil, ela segue a lógica do processo penal comum, mas adaptada ao ambiente virtual.

Nesse sentido, a apuração é conduzida primordialmente pela polícia judiciária, sob supervisão do Ministério Público e, quando necessário, com autorização do Poder Judiciário. Nesse cenário, é relevante mencionar o artigo 5º, inciso XII, da Constituição Federal de 1988, que assegura a inviolabilidade das comunicações, permitindo sua quebra apenas por ordem judicial. Esse dispositivo estabelece o equilíbrio entre a proteção da privacidade e a necessidade de efetividade da investigação penal.

Ademais, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, reforça esse entendimento em seu artigo 15, que impõe às plataformas digitais o dever de manter, pelo prazo mínimo de seis meses, registros de acesso capazes de identificar usuários. Esse dispositivo possibilita que, mesmo sem acesso imediato ao conteúdo de mensagens privadas, a autoridade policial consiga rastrear o responsável por determinada conduta. Em complemento, o artigo 22 da mesma lei estabelece a possibilidade de o juiz determinar a guarda e disponibilização de tais registros, constituindo a base jurídica para a quebra de sigilo digital no país.

Após examinar os dispositivos e normas indispensáveis para a efetivação das investigações, é importante compreender como se dá a aplicação prática dessas previsões legais. O procedimento divide-se em etapas: inicia-se com a notícia do crime, geralmente proveniente de denúncias de vítimas, do monitoramento aberto de conteúdos públicos ou de relatórios de plataformas. Cumpre destacar que esse monitoramento não é aleatório, pois, se fosse, violaria o art. 5º, XII, da Constituição. Na prática, a vigilância pode decorrer de uma denúncia formal ou ainda do acompanhamento de espaços públicos da internet, como fóruns abertos, redes sociais públicas e convites de servidores.

Em seguida, as autoridades solicitam, quando necessário, ordem judicial para a quebra de sigilo de registros ou comunicações privadas. Uma vez deferida a medida, os dados são fornecidos pelas empresas responsáveis, podendo ainda demandar cooperação internacional. Após a análise técnica do material obtido, o Ministério Público pode oferecer a denúncia.

3. Análise a respeito do limite da investigação sobre a privacidade

De acordo com Patrícia Peck Pinheiro, uma das maiores autoras e especialistas em Direito Digital e Cibersegurança, “a persecução penal em meios digitais exige equilíbrio: não se pode permitir que a privacidade seja utilizada como escudo para práticas ilícitas, ao mesmo tempo em que o monitoramento estatal deve respeitar garantias constitucionais” (PECK, 2021, p. 87).

Com base nessa afirmação, é evidente a necessidade de uma fiscalização mais rigorosa do Estado em casos extremos como o exemplo mencionado, pois é imperioso que nenhum ato ilícito permaneça impune, independentemente de onde ou quando tenha sido praticado. Nesse sentido, também não se deve atrasar o processo legal por meio de “escudos jurídicos” sustentados por leis que, a priori, foram promulgadas para garantir a segurança da população nas redes.

É igualmente claro que é essencial assegurar os direitos fundamentais estabelecidos pela Constituição Federal. No entanto, com o avanço tecnológico, observa-se uma evolução natural desses direitos. Nesse viés, cabe ao Estado adaptar-se à realidade digital contemporânea, garantindo não apenas a segurança informacional, mas também a integridade psicológica e moral dos usuários da internet no Brasil.

Portanto, a privacidade é assegurada pela Constituição Federal desde 1988 e reforçada, no âmbito tecnológico, por leis como a LGPD. Contudo, como demonstrado, esse direito pode

ser relativizado em casos de investigação criminal, nos quais o Estado deve ter acesso adequado às evidências, sempre com ênfase na celeridade do procedimento para alcançar resultados efetivos.

4. Conclusão

A análise realizada demonstra que a privacidade digital, embora reconhecida como direito fundamental e reforçada por legislações nacionais e internacionais, não é absoluta. O ordenamento jurídico brasileiro busca harmonizar a proteção da intimidade dos cidadãos com a necessidade de eficácia das investigações criminais no ambiente virtual. Normas como o Marco Civil da Internet e a LGPD evidenciam essa dualidade: ao mesmo tempo em que garantem direitos, também estabelecem mecanismos que permitem, sob controle judicial, o acesso a dados indispensáveis para a persecução penal.

Assim, a validação da privacidade para fins de investigação deve ser compreendida como um instrumento de equilíbrio. Não se trata de suprimir garantias individuais, mas de compatibilizá-las com a realidade digital e com a proteção da coletividade. Nesse contexto, o desafio do Estado consiste em assegurar a efetividade das investigações sem transformar a tutela da privacidade em barreira à justiça, mas, sim, em elemento de um processo democrático que respeita direitos e promove segurança jurídica e social.

REFERÊNCIAS

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

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Diário Oficial da União: seção 1, Rio de Janeiro, 31 dez. 1940

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018

8, de 7 de dezembro de 1940 – Código Penal. Diário Oficial da União: seção 1, Brasília, DF, 27 dez. 2019

CONSELHO DA EUROPA. **Convenção nº 108 para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados de Caráter Pessoal**, de 28 de janeiro de 1981. Estrasburgo, 1981. (Atualizada pelo Protocolo de 2018 – Convenção 108

PECK PINHEIRO, Patrícia. *Direito Digital*. 8. ed. São Paulo: Saraiva, 2021.