

HILDA MARIA RODRIGUES MONTEIRO

**UM ESTUDO SOBRE A LEI CAROLINA DIECKMANN (LEI 12.737/2012):
INOVAÇÃO LEGISLATIVA E SEUS DESDOBRAMENTOS NA ERA DA
INFORMAÇÃO**

TERESINA-PI 2025

HILDA MARIA RODRIGUES MONTEIRO

**UM ESTUDO SOBRE A LEI CAROLINA DIECKMANN (LEI 12.737/2012):
INOVAÇÃO LEGISLATIVA E SEUS DESDOBRAMENTOS NA ERA DA
INFORMAÇÃO**

Trabalho de Conclusão de Curso
apresentado à Afya Centro Universitário –
Uninovafapi, para obtenção do título de
Bacharel em Direito.

Orientador(a): Prof.a. Me: Enedina Gizeli
Albano Moura.

TERESINA – PI 2025

FICHA CATALOGRÁFICA

M775e Monteiro, Hilda Maria Rodrigues.

Um estudo sobre a Lei Carolina Dieckmann (LEI 12.737/2012): inovação legislativa e seus desdobramentos na era da informação / Hilda Maria Rodrigues Monteiro – Teresina: UNINOVAFAPI, 2025.

Orientador (a): Profº. Ma. Enedina Gizeli Albano Moura – UNINOVAFAPI, 2025.

31.p.; 23cm.

Trabalho de conclusão (Graduação em Direito) – UNINOVAFAPI, Teresina, 2025.

1. Lei Carolina Dieckmann. 2. Crimes cibernéticos. 3. Privacidade. 4. Segurança da informação. 5. Direito penal digital. I. Título. II. Monteiro, Hilda Maria Rodrigues.

CDD 345.026 8

Catálogo na publicação
Francisco Renato Sampaio da Silva – CRB/1028

HILDA MARIA RODRIGUES MONTEIRO

**UM ESTUDO SOBRE A LEI CAROLINA DIECKMANN (LEI 12.737/2012):
Inovação Legislativa e seus desdobramentos na era da
Informação**

Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do
Afya Centro Universitário Uninovafapi,
como requisito parcial para obtenção do
grau de Bacharel em Direito.

Data de Aprovação: 10 / 11 / 2025

BANCA EXAMINADORA

Enedina Gileli Albano Moura

Professora Mestra Enedina Albano Moura
Afya Centro Universitário Uninovafapi
(Orientadora)

Vanessa Nunes de Barros Mendes Sampaio

Professora Mestra Vanessa Nunes de Barros Mendes Sampaio
Afya Centro Universitário Uninovafapi
(1º Examinador)

Ana Carolina Barros e Silva

Professora Mestra Ana Carolina Barros e Silva
Centro Universitário Tecnológico de Teresina – UNICET
(2º Examinador)

Aos meus pais e minha irmã que foram luz em meus dias

Tormento!

Dedico!

AGRADECIMENTOS

A minha orientadora, prof.(a). Me.Enedina Gizeli Albano Moura que, durante a trajetória deste trabalho foi suporte em todo desenvolvimento de pesquisa, orientando, auxiliando de forma que os objetivos deste trabalho fossem bem instruídos.

Aos meus pais Hildo Gomes Monteiro e Antônia Maria Rodrigues Monteiro,minha irmã Yasmin Rodrigues Monteiro e a minha madrinha Maria Edna Gomes Monteiro que foram acima de tudo a base e força para que concluísse essa minha jornada. Ao meu namorado que apesar de tudo, foi a luz, minha alegria e minha motivação em dias árduos.

Por fim, agradeço a todos que, durante toda minha jornada puderam de certa forma auxiliar, motivar e cooperar para que a realização deste trabalho fosse concluído.

RESUMO

O trabalho analisa a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, criada após o caso de invasão e divulgação de fotos da atriz homônima, como resposta à necessidade de criminalizar condutas praticadas no ambiente digital. A lei representa um marco na tutela penal contra crimes cibernéticos no Brasil, introduzindo os artigos 154-A e 154-B no Código Penal, que tratam da invasão de dispositivos informáticos e da proteção da privacidade e da segurança da informação. Apesar de seu caráter inovador, a pesquisa demonstra que a norma possui limitações, pois não abrange modalidades modernas de cibercrime, como phishing, ransomware e fraudes eletrônicas sem invasão direta. O estudo destaca que a efetividade da lei depende de constante atualização legislativa, da cooperação internacional e do fortalecimento da investigação digital. Também analisa o papel complementar de outras normas, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), que, juntamente com a Lei Carolina Dieckmann, compõem o tripé jurídico de proteção da privacidade no Brasil. Conclui-se que, embora tenha sido um avanço significativo, a legislação ainda carece de abrangência e integração para enfrentar os desafios da era digital, sendo necessária uma política pública que una repressão penal, educação digital e conscientização social para garantir uma proteção efetiva dos direitos fundamentais no ciberespaço.

Palavras-chave: Lei Carolina Dieckmann; Crimes Cibernéticos; Privacidade; Segurança da Informação; Direito Penal Digital.

ABSTRACT

This paper analyzes Law No. 12,737/2012, known as the Carolina Dieckmann Law, created after the case of the invasion and dissemination of photos of the actress of the same name, as a response to the need to criminalize conduct practiced in the digital environment. The law represents a milestone in criminal protection against cybercrimes in Brazil, introducing articles 154-A and 154-B into the Penal Code, which deal with the invasion of computer devices and the protection of privacy and information security. Despite its innovative nature, the research demonstrates that the law has limitations, as it does not cover modern forms of cybercrime, such as phishing, ransomware, and electronic fraud without direct invasion. The study highlights that the effectiveness of the law depends on constant legislative updates, international cooperation, and the strengthening of digital investigation. It also analyzes the complementary role of other norms, such as the Marco Civil da Internet (Brazilian Internet Bill of Rights) and the Lei Geral de Proteção de Dados (LGPD) (Brazilian General Data Protection Law), which, together with the Carolina Dieckmann Law, make up the legal tripod of privacy protection in Brazil. It is concluded that, although it was a significant step forward, the legislation still lacks the scope and integration to face the challenges of the digital age, and a public policy is needed that unites criminal repression, digital education and social awareness to guarantee effective protection of fundamental rights in cyberspace.

Keywords: Carolina Dieckmann Law; Cybercrimes; Privacy; Information Security; Digital Criminal Law.

SUMÁRIO

1 INTRODUÇÃO	10
2 ANÁLISE CRÍTICA DA LEI CAROLINA DIECKMANN.....	12
3 TIPIFICAÇÃO PENAL E CONDUTAS PREVISTAS	16
3.1 A Era Digital e os desafios da segurança da informação	19
4 EFETIVIDADE E DESAFIOS DA LEI CAROLINA DIECKMANN NA PROTEÇÃO PENAL	24
CONTRA CRIMES CIBERNÉTICOS.....	24
5 CONCLUSÃO	25
REFERÊNCIAS.....	27
 ANEXO A	 31

1 INTRODUÇÃO

O presente trabalho tem como foco analisar a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que representa um marco na consolidação da tutela penal voltada aos crimes cibernéticos no Brasil. A promulgação dessa lei, como afirmam Caleffi e Neto (2013), resultou de um episódio amplamente divulgado pela mídia envolvendo a atriz Carolina Dieckmann, que teve seu computador invadido e suas fotos íntimas publicadas sem autorização. O caso ganhou grande repercussão social e impulsionou o debate sobre a necessidade de uma legislação específica para punir as invasões de dispositivos informáticos, culminando na aprovação da referida norma em tempo recorde.

Com o avanço tecnológico e a popularização da internet, as relações sociais, econômicas e jurídicas passaram a se desenvolver também no ambiente digital, o que trouxe benefícios e desafios à sociedade contemporânea. Segundo Nascimento (2016), essa transformação gerou novas formas de vulnerabilidade e criminalidade, exigindo do Estado respostas mais rápidas e adequadas à complexidade dos delitos informáticos. Antes da promulgação da Lei Carolina Dieckmann, o ordenamento jurídico brasileiro não dispunha de dispositivos capazes de punir adequadamente a invasão de sistemas e o furto de dados pessoais, o que deixava um vácuo legal diante da crescente criminalidade virtual.

De acordo com Alcântara (2022), a Lei nº 12.737/2012 inaugurou uma nova etapa na proteção penal de direitos fundamentais como a privacidade e a inviolabilidade das comunicações, previstos no artigo 5º da Constituição Federal de 1988 (Brasil, 1988). Apesar de sua relevância histórica, a autora ressalta que a norma possui limitações práticas, uma vez que se mostra restrita diante da diversidade de crimes digitais existentes. Na mesma linha, Prazeres (2013) argumenta que o texto

legal é pontual e não abrange modalidades como phishing, ransomware e fraudes eletrônicas sem invasão direta de dispositivos, o que demonstra a necessidade de atualização constante da legislação penal frente às novas formas de criminalidade digital.

O problema central deste estudo consiste em analisar em que medida a Lei Carolina Dieckmann é eficaz no combate aos crimes cibernéticos e quais são seus limites diante da rápida evolução tecnológica e das transformações da sociedade da informação. Conforme observa Meirelles (2020), o avanço das tecnologias digitais trouxe consigo a expansão de condutas criminosas que desafiam a aplicação das leis tradicionais, demandando um sistema normativo mais abrangente e adaptável.

O objetivo geral da pesquisa é examinar a aplicabilidade e efetividade da Lei nº 12.737/2012 no contexto atual, enquanto os objetivos específicos buscam compreender o processo de sua criação, suas principais tipificações penais e as limitações práticas que dificultam a repressão dos delitos digitais. Nesse sentido, o estudo também dialoga com outras legislações correlatas, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018), que, conforme destacam Machado e Duarte (2021), formam, em conjunto, o tripé normativo de proteção jurídica da privacidade e da segurança digital no Brasil.

A metodologia utilizada é de caráter qualitativo e bibliográfico, fundamentada em obras doutrinárias, legislações e estudos científicos. Foram consideradas contribuições de autores como Dantas (2017), Nascimento (2016), Furlan (2019), Silva (2020) e Guimarães (2024), que discutem a evolução da tutela penal dos crimes digitais e a necessidade de integração entre tecnologia, investigação e Direito. De acordo com Meirelles (2020), o enfrentamento eficaz da criminalidade virtual exige o fortalecimento da cooperação internacional e o aprimoramento das técnicas periciais, dado que muitos delitos cibernéticos são transnacionais e envolvem anonimato e complexidade técnica.

A justificativa para o desenvolvimento deste trabalho encontra respaldo na relevância social e jurídica da temática, considerando o aumento expressivo dos crimes cibernéticos e a fragilidade estrutural da segurança digital no Brasil. Dados do relatório FortiGuard Labs (2022) revelam que o país figura entre os que mais sofrem ataques cibernéticos no mundo, o que evidencia a urgência de políticas públicas de

prevenção, educação digital e modernização legislativa. Para Bezerra (2019) e Castro (2021), a proteção da informação ultrapassa a esfera técnica, alcançando dimensões éticas, sociais e jurídicas, sendo indispensável que o Estado e a sociedade estejam preparados para lidar com os riscos da era digital.

Dessa forma, o presente estudo busca contribuir para o debate acadêmico e jurídico acerca da eficácia da Lei Carolina Dieckmann, examinando seus impactos, limites e perspectivas de aprimoramento. A análise evidencia que o combate aos crimes cibernéticos demanda não apenas instrumentos penais adequados, mas também educação digital, conscientização social e cooperação internacional, elementos indispensáveis para a consolidação de um ambiente digital seguro e para a proteção efetiva dos direitos fundamentais na era da informação.

2 ANÁLISE CRÍTICA DA LEI CAROLINA DIECKMANN

A promulgação da Lei nº 12.737/2012, conhecida popularmente como Lei Carolina Dieckmann, representou um marco na evolução da legislação penal brasileira, ao inaugurar o tratamento jurídico específico dos crimes cibernéticos. A criação dessa norma está intrinsecamente relacionada ao avanço da tecnologia e à popularização da internet no Brasil, fenômenos que transformaram a comunicação, o trabalho e as relações pessoais, mas também ampliaram o espaço para a prática de delitos de natureza digital.

Até o início da década de 2010, o ordenamento jurídico brasileiro não possuía dispositivos legais capazes de punir adequadamente a invasão de dispositivos informáticos, o furto de dados pessoais e a divulgação de informações privadas obtidas por meios ilícitos. Essa lacuna tornava inviável a responsabilização penal de agentes que cometessem crimes através da rede, uma vez que as condutas não se enquadravam de forma precisa em tipos penais já existentes. Conforme observa Lucas Sousa do Nascimento (2016), a ausência de previsão legal para tais situações expunha a fragilidade do sistema jurídico diante do rápido avanço tecnológico, criando um descompasso entre a realidade social e a resposta estatal.

Foi nesse contexto que ocorreu o caso da atriz Carolina Dieckmann, em maio de 2012. Seu computador pessoal foi invadido por hackers, e 36 fotografias íntimas foram copiadas e posteriormente divulgadas na internet sem sua autorização. O episódio ganhou ampla repercussão na mídia nacional e internacional, despertando uma forte comoção pública e levantando debates sobre a violação de privacidade e a

impunidade de crimes digitais (Caleffi; Neto, 2013). A cobertura jornalística intensa, especialmente pela televisão, contribuiu para que o caso se tornasse símbolo da necessidade urgente de regulamentação penal específica para delitos informáticos.

A partir da repercussão do caso, um projeto de lei que já tramitava no Congresso Nacional desde 2011, o Projeto de Lei nº 2.793/2011, ganhou prioridade. O texto propunha a criminalização da invasão de dispositivos eletrônicos com o intuito de obter, adulterar ou destruir dados sem autorização. Em virtude da pressão social e política gerada pela exposição do caso, o projeto foi votado de forma acelerada. Conforme destacam Caleffi e Neto (2013), o trâmite que normalmente levaria meses foi concluído em apenas doze dias: aprovado pela Câmara dos Deputados, seguiu ao Senado e foi sancionado pela então presidente da República, Dilma Rousseff, em 30 de novembro de 2012.

A Lei nº 12.737/2012 alterou o Código Penal Brasileiro ao incluir os artigos 154A e 154-B, estabelecendo pena de três meses a um ano de detenção e multa para quem invadir dispositivo informático alheio, com o objetivo de obter, adulterar ou destruir dados ou informações sem autorização do titular. Além disso, a pena é agravada quando houver divulgação, comercialização ou transmissão a terceiros das informações obtidas por meio da invasão (Brasil, 2012). Essa inovação legislativa representou um avanço significativo na proteção dos direitos fundamentais à intimidade, à privacidade e à inviolabilidade das comunicações, princípios previstos no artigo 5º da Constituição Federal de 1988.

A criação da Lei Carolina Dieckmann é frequentemente citada como exemplo do chamado “populismo punitivo”, conceito que, segundo Nascimento (2016), refere-se à tendência de criação de leis penais em resposta direta ao clamor social, frequentemente impulsionado pela mídia. Assim, mais do que uma resposta técnica à realidade dos crimes digitais, a norma também refletiu o contexto político-criminal brasileiro contemporâneo, caracterizado pela rápida produção de leis penais em momentos de forte mobilização popular. Ainda que tenha sido motivada por um caso isolado, sua promulgação atendeu à demanda por um endurecimento das respostas penais, reforçando o papel simbólico do Direito Penal como instrumento de controle social e de apaziguamento de tensões públicas.

Do ponto de vista técnico, a nova lei apresentou avanços e limitações. Segundo Prazeres (2013), apesar de representar um progresso jurídico, a redação da norma

mostrou-se insuficiente para abarcar a complexidade dos delitos cibernéticos, já que não alcança, por exemplo, ataques realizados a sistemas de empresas públicas ou privadas, fraudes eletrônicas e crimes de disseminação em massa de dados pessoais. Essa limitação fez com que especialistas classificassem a lei como pontual e restrita, uma vez que seu foco recaiu quase exclusivamente sobre a invasão de dispositivos individuais, deixando de lado outras modalidades de crimes virtuais.

Em perspectiva histórica, a Lei Carolina Dieckmann marcou o início da criminalização formal dos delitos informáticos no Brasil, representando um primeiro passo em direção a um arcabouço jurídico mais abrangente para o ambiente digital.

Sua promulgação reforçou a ideia de que o Estado deve acompanhar as transformações tecnológicas e garantir a tutela penal de bens jurídicos que, na era digital, assumem novas formas e valores. Conforme observa Nascimento (2016), embora tenha nascido em meio a um episódio de grande apelo midiático, a norma serviu como porta de entrada para discussões mais amplas sobre a proteção de dados, segurança cibernética e responsabilidade digital.

Portanto, a Lei nº 12.737/2012 simboliza não apenas uma resposta ao caso de violação sofrido por uma figura pública, mas também a consolidação do reconhecimento dos crimes cibernéticos como uma realidade jurídica e social no Brasil. Sua origem revela o poder de influência da mídia na formulação de políticas criminais e a necessidade de o legislador equilibrar a resposta penal entre a demanda popular e a técnica jurídica. Em síntese, o diploma legal resultou de uma combinação entre o avanço tecnológico, o clamor social e o interesse político, abrindo caminho para uma nova fase de debate sobre a privacidade e a proteção jurídica no ambiente digital brasileiro.

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, integra um conjunto mais amplo de normas que compõem o marco jurídico da segurança digital no Brasil, ao lado do Marco Civil da Internet (Lei nº 12.965/2014) e da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Essas legislações, embora tenham surgido em momentos distintos e com objetivos específicos, formam um sistema jurídico complementar voltado à prevenção, proteção e repressão das condutas ilícitas praticadas no ambiente virtual (Machado; Duarte, 2021).

A Lei Carolina Dieckmann foi a primeira norma penal a tipificar de forma direta a invasão de dispositivos informáticos, criminalizando condutas de acesso indevido,

adulteração e divulgação de dados pessoais sem consentimento. Conforme apontam Machado e Duarte (2021), o diploma legal, ainda que restrito, inaugurou uma nova fase de reconhecimento dos delitos cibernéticos, impulsionando o avanço normativo sobre a proteção da privacidade e dos dados pessoais.

Em sequência, o Marco Civil da Internet, sancionado em 2014, instituiu os princípios, garantias, direitos e deveres para o uso da internet no Brasil. De acordo com o artigo 7º, o Marco Civil assegura a inviolabilidade da intimidade e da vida privada, bem como a proteção dos dados pessoais e o sigilo das comunicações, sendo considerado a “Constituição da Internet” (Brasil, 2014). Para Nunes e Madrid (2019), o Marco Civil representou um avanço na consolidação dos direitos digitais, ao estabelecer bases jurídicas para a responsabilização de provedores e garantir maior transparência no tratamento de dados pelos agentes da rede.

Posteriormente, a Lei Geral de Proteção de Dados (LGPD), promulgada em 2018, consolidou a proteção da privacidade e dos dados pessoais como um direito fundamental. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD regula o tratamento de informações pessoais tanto por entidades públicas quanto privadas, impondo limites ao uso indevido de dados e prevendo sanções administrativas em casos de descumprimento (Cots; Oliveira, 2018). De acordo com Machado e Duarte (2021), a LGPD, em conjunto com a Lei Carolina Dieckmann, reforça a responsabilidade civil e administrativa no âmbito digital, ainda que sua atuação penal seja limitada.

Esse tripé normativo, Lei Carolina Dieckmann, Marco Civil da Internet e LGPD, reflete o esforço do Estado brasileiro em construir uma estrutura jurídica sólida para lidar com os desafios da cibersociedade, buscando equilibrar o avanço tecnológico com a preservação dos direitos fundamentais. Como observa Damasceno (2019), tais leis, embora complementares, ainda carecem de efetividade prática, especialmente no que tange à investigação e punição de crimes cibernéticos, em razão da constante evolução tecnológica e da complexidade das redes digitais.

No âmbito internacional, destaca-se a Convenção de Budapeste sobre o Cibercrime, firmada em 2001 pelo Conselho da Europa. Esse tratado é o primeiro instrumento jurídico internacional voltado ao combate dos crimes cibernéticos, estabelecendo parâmetros para a cooperação entre os Estados, a harmonização das legislações internas e o fortalecimento da investigação transnacional. Segundo

Pinheiro (2006), a Convenção de Budapeste serviu como modelo para diversos países, inclusive para o Brasil, que, embora não seja signatário formal, utiliza seus princípios como referência para o aprimoramento da política criminal no ciberespaço.

A influência da Convenção de Budapeste é perceptível nas legislações brasileiras posteriores, especialmente na ênfase à cooperação jurídica internacional, à proteção de dados e à criminalização de condutas específicas relacionadas à invasão de sistemas e interceptação ilícita de informações. Como destacam Padovez e Prado (2019), a experiência internacional reforça a importância de o Brasil avançar em políticas públicas integradas e de atualização constante das normas, de modo a assegurar a efetividade da repressão penal e da proteção digital.

Dessa forma, o marco normativo brasileiro e internacional revela um processo de evolução legislativa e institucional que acompanha o crescimento dos riscos cibernéticos e a crescente dependência da sociedade digital. Apesar de avanços significativos, autores como Machado e Duarte (2021) e Damasceno (2019) apontam que ainda há necessidade de integração entre os mecanismos de prevenção, responsabilização e educação digital, a fim de garantir uma proteção jurídica mais ampla e eficaz frente às novas formas de criminalidade virtual.

3 TIPIFICAÇÃO PENAL E CONDUTAS PREVISTAS

A evolução tecnológica trouxe inúmeros benefícios à sociedade contemporânea, mas também originou novas formas de criminalidade que desafiam o Direito Penal tradicional. Entre essas novas modalidades, destacam-se os crimes cibernéticos, que atentam diretamente contra a privacidade, a segurança da informação e outros direitos fundamentais dos cidadãos. Diante desse cenário, o legislador brasileiro editou a Lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, que incluiu os artigos 154-A e 154-B no Código Penal Brasileiro, visando coibir condutas ilícitas praticadas por meio eletrônico e digital.

De acordo com Alcântara (2022), essa lei foi um marco na história legislativa nacional, pois reconheceu formalmente a necessidade de tutelar penalmente a violação de dispositivos informáticos e a obtenção não autorizada de dados pessoais. A autora observa que a criação da norma foi motivada pela exposição indevida de dados íntimos de uma figura pública, o que revelou a vulnerabilidade dos cidadãos no ambiente digital. A partir desse episódio, o Estado percebeu a urgência de estabelecer

parâmetros penais para punir invasões de privacidade no ciberespaço, protegendo o indivíduo de danos morais e materiais resultantes dessas práticas.

O artigo 154-A do Código Penal, incluído pela referida lei, define como crime a invasão de dispositivo informático alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados e informações sem autorização expressa do titular, ou de instalar vulnerabilidades para obter vantagem ilícita. A pena prevista é de detenção de três meses a um ano e multa, podendo ser aumentada de um sexto a um terço se houver divulgação, comercialização ou transmissão a terceiros dos dados obtidos. Esse tipo penal busca coibir o comportamento invasivo e garantir a segurança dos sistemas de informação, que se tornaram essenciais à vida moderna (Brasil, 2012).

Já o artigo 154-B estabelece que a ação penal é pública condicionada à representação da vítima, salvo quando o crime for cometido contra a administração pública direta ou indireta, incluindo autarquias, empresas públicas e sociedades de economia mista, hipótese em que a ação será pública incondicionada. Essa disposição reflete o princípio da intervenção mínima do Direito Penal, uma vez que o Estado só atua mediante provocação do ofendido quando o bem jurídico afetado é de natureza privada. Por outro lado, quando o ataque cibernético compromete interesses públicos ou institucionais, o Estado deve agir de ofício, em razão do interesse coletivo envolvido (Tourinho Filho, 2010).

O bem jurídico tutelado pelos dispositivos em questão é a privacidade e a segurança da informação, direitos assegurados constitucionalmente. O artigo 5º, inciso X, da Constituição Federal, protege a intimidade, a vida privada e a imagem das pessoas, assegurando indenização pelo dano moral ou material decorrente de sua violação. Já o inciso LXXIX, introduzido pela Emenda Constitucional nº 115/2022, consagrou expressamente a proteção dos dados pessoais, inclusive nos meios digitais, como direito fundamental, reforçando a importância da tutela da informação como expressão da dignidade humana (Brasil, 1988).

Conforme observa Patrícia Peck Pinheiro (2020), a proteção da privacidade digital representa um dos maiores desafios do século XXI, pois o avanço tecnológico supera, em ritmo acelerado, a capacidade de resposta do Estado. A autora destaca que a Lei nº 12.737/2012 foi uma resposta inicial, mas ainda limitada, diante da complexidade dos delitos cibernéticos e da diversidade de condutas que ameaçam a

integridade das informações digitais. Segundo ela, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) complementou a tutela jurídica ao estabelecer regras sobre coleta, armazenamento e compartilhamento de informações pessoais, integrando o sistema normativo de proteção da privacidade.

Além disso, Rossini (2004) afirma que o chamado delito informático consiste em qualquer conduta ilícita, dolosa ou culposa, praticada mediante o uso de recursos tecnológicos, que afete direta ou indiretamente a segurança informática, cuja integridade, disponibilidade e confidencialidade constituem os seus principais elementos. Nessa perspectiva, o artigo 154-A do Código Penal cumpre o papel de coibir a violação de um bem jurídico coletivo e difuso, pois a segurança das redes e dos sistemas é um valor indispensável à confiança digital e à ordem social contemporânea.

Por sua vez, Teixeira (2019) acrescenta que a dificuldade na aplicação da Lei Carolina Dieckmann está na coleta e produção de provas digitais, uma vez que a natureza volátil dos dados e a facilidade de anonimato dificultam a identificação dos autores. Segundo o autor, o avanço das técnicas de investigação e o treinamento especializado dos agentes públicos são essenciais para garantir a efetividade da lei e evitar que sua aplicação se restrinja ao plano teórico.

Outro ponto relevante é a cooperação internacional. Em razão da natureza global da internet, muitos crimes informáticos são praticados a partir de servidores localizados fora do território nacional, o que exige a aplicação de tratados internacionais de cooperação jurídica e mecanismos de auxílio mútuo entre Estados. A Convenção de Budapeste sobre o Cibercrime (2001), ratificada pelo Brasil em 2021, representa um marco nesse sentido, ao promover a uniformização das normas e procedimentos voltados à repressão de crimes cibernéticos em escala global (Convenção de Budapeste, 2001).

Em síntese, a Lei nº 12.737/2012 constitui um avanço relevante na proteção da privacidade e da segurança da informação, reforçando o compromisso do Estado brasileiro com a tutela dos direitos fundamentais em ambiente digital. Contudo, conforme salientam Alcântara (2022) e Pinheiro (2020), sua eficácia depende de uma política pública abrangente que envolva educação digital, modernização das estruturas investigativas e integração normativa com a Lei Geral de Proteção de Dados e demais instrumentos internacionais de combate ao cibercrime. Dessa forma,

a efetividade da norma vai além da simples punição penal, estendendo-se à construção de uma cultura de segurança cibernética e respeito à privacidade como pilares da cidadania digital.

3.1 A Era Digital e os desafios da segurança da informação

A era digital transformou profundamente a forma como as pessoas interagem, consomem, produzem e compartilham informações. Se por um lado os avanços tecnológicos proporcionaram eficiência, conectividade e inovação em diversos setores, por outro trouxeram novos riscos à segurança da informação e à privacidade dos usuários. Conforme ressaltam Casotti et al. (2024), o crescimento exponencial das atividades digitais impulsionadas por redes sociais, serviços online e plataformas de armazenamento em nuvem ampliou significativamente a exposição de dados pessoais e corporativos, tornando a segurança digital uma questão central para o direito e a cidadania contemporânea.

Com o uso massivo das redes sociais, as fronteiras entre o público e o privado tornaram-se cada vez mais difusas. A facilidade de compartilhar informações em ambientes digitais gera vulnerabilidades que são exploradas por ataques cibernéticos, fraudes eletrônicas e práticas de engenharia social, comprometendo a integridade e a confiabilidade dos dados. Nesse sentido, Mendes (2019) observa que a digitalização da vida cotidiana exige um novo paradigma jurídico baseado na prevenção e na responsabilização, pois o sistema jurídico tradicional não foi originalmente projetado para lidar com crimes de natureza virtual.

Segundo Doneda (2019), a privacidade e a proteção de dados pessoais deixaram de ser apenas direitos individuais e passaram a constituir direitos fundamentais de quarta geração, relacionados à autonomia e à dignidade humana. Essa mudança reflete a necessidade de reconhecer os dados pessoais como bens jurídicos dotados de valor econômico e simbólico, cuja tutela requer mecanismos normativos específicos. Nesse contexto, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) surge como instrumento essencial para regular o tratamento de dados e proteger o indivíduo diante do poder informacional de grandes corporações e agentes públicos.

A modernização das relações sociais pela internet trouxe também um desafio global: como equilibrar o avanço tecnológico com a segurança jurídica e a proteção

de direitos fundamentais. Conforme observa Castro (2021), garantir segurança jurídica na era digital exige uma postura proativa, baseada em constante atualização legislativa e na cooperação internacional entre Estados. Essa perspectiva é corroborada por Casotti et al. (2024), que destacam que o Brasil vem aprimorando seu arcabouço normativo com leis como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei nº 14.155/2021, que agravou as penas para crimes cibernéticos, reforçando a importância da legislação penal como instrumento de dissuasão.

Além das questões jurídicas, a educação digital surge como pilar fundamental para o fortalecimento da segurança informacional. Bezerra (2019) salienta que o desconhecimento dos usuários sobre as vulnerabilidades dos sistemas digitais é um dos principais fatores que contribuem para a ocorrência de golpes e fraudes online. Assim, a segurança da informação não deve ser compreendida apenas como um problema técnico, mas também ético, social e educacional, que demanda conscientização coletiva e políticas públicas eficazes.

Outro ponto relevante é a dimensão econômica da informação. Mendes (2019) enfatiza que os dados pessoais se tornaram um dos ativos mais valiosos do século XXI, utilizados para fins comerciais, políticos e estratégicos. Por isso, a proteção desses dados é condição essencial para garantir a confiança nas relações digitais e preservar a livre concorrência e a segurança jurídica no ambiente virtual.

Em síntese, os desafios da era digital não se limitam à criação de normas, mas à implementação efetiva de mecanismos de governança da informação, capazes de equilibrar inovação, privacidade e segurança. A LGPD, o Marco Civil da Internet e outras normas correlatas compõem o alicerce de um sistema de proteção ainda em construção, que precisa acompanhar as transformações tecnológicas em ritmo constante. Como conclui Casotti et al. (2024), a segurança da informação é um dos pilares da confiança digital e da preservação dos direitos fundamentais, sendo indispensável o compromisso conjunto entre Estado, empresas e sociedade civil para consolidar um ambiente digital seguro, transparente e ético.

Desde os primeiros registros de delitos digitais, ocorridos na década de 1960, a criminalidade no ambiente virtual passou por um processo de sofisticação sem precedentes. O que antes se limitava a simples práticas de espionagem eletrônica e sabotagem de sistemas, evoluiu para fraudes financeiras complexas, ataques de ransomware e crimes de engenharia social altamente elaborados. Segundo Meirelles

(2020), a era digital inaugurou uma nova fase de criminalidade, marcada pela globalização da informação e pela facilidade de acesso a tecnologias que permitem a prática de condutas ilícitas à distância, tornando o Direito Penal um instrumento essencial para a proteção dos bens jurídicos no ambiente virtual.

Durante a pandemia de Covid-19, esse cenário tornou-se ainda mais preocupante. O isolamento social e a digitalização de atividades econômicas, educacionais e profissionais criaram um terreno fértil para o crescimento exponencial de ataques cibernéticos. De acordo com o relatório FortiGuard Labs (2022), o Brasil registrou cerca de 31,5 milhões de tentativas de ataques cibernéticos, número que revela a urgência de políticas públicas e instrumentos penais eficazes para coibir tais práticas. A vulnerabilidade digital não se restringe às instituições privadas, alcançando também os órgãos públicos, como observado nos ataques a tribunais e sistemas governamentais, que evidenciam a fragilidade estrutural da cibersegurança nacional.

A transnacionalidade e o anonimato são fatores que dificultam significativamente a investigação e punição dos responsáveis. Conforme aponta Silva (2020), a ausência de fronteiras físicas no ambiente virtual e a possibilidade de mascarar identidades desafiam os mecanismos tradicionais de persecução penal, tornando necessária uma cooperação jurídica internacional mais efetiva. A autora destaca que o cibercrime não respeita jurisdições, exigindo uma resposta coordenada entre os Estados, inspirada em instrumentos como a Convenção de Budapeste sobre o Cibercrime (2001), que estabelece diretrizes globais para a tipificação e investigação de crimes digitais.

Nesse contexto, Meirelles (2020) ressalta que o Direito Penal contemporâneo precisa se adaptar à nova realidade tecnológica, reconhecendo que a criminalidade digital atinge não apenas bens materiais, mas também valores fundamentais como a privacidade, a honra e a segurança da informação. A autora propõe uma releitura da função preventiva do Direito Penal, voltada para a proteção da dignidade humana no ambiente digital e para o fortalecimento da confiança dos cidadãos nas interações virtuais.

Autores como Alexandre (2023) e Guimarães (2024) reforçam que o combate aos crimes cibernéticos deve ir além da simples punição, abrangendo a capacitação técnica de agentes públicos, a educação digital da população e a atualização constante da legislação penal. Alexandre (2023) observa que a efetividade da tutela

penal depende da integração entre as esferas jurídica e tecnológica, especialmente no que se refere à produção de provas digitais e à rastreabilidade de condutas ilícitas. Já Guimarães (2024) sustenta que a prevenção é o principal caminho para conter o avanço do cibercrime, sendo essencial o investimento em alfabetização digital, para que os usuários compreendam os riscos do compartilhamento de dados e adotem práticas seguras no ciberespaço.

A análise de Meirelles (2020) também enfatiza que o anonimato virtual oferece uma falsa sensação de impunidade, estimulando condutas criminosas como injúrias, difamações, extorsões e estelionatos eletrônicos, o que exige uma resposta penal proporcional e moderna. Assim, a tutela penal deve ser compreendida como um instrumento de garantia da ordem digital, voltado a equilibrar a liberdade de expressão e o direito à privacidade, de modo a preservar os fundamentos do Estado Democrático de Direito também no ambiente virtual.

Portanto, diante da complexidade dos crimes cibernéticos, é imprescindível que o Direito Penal brasileiro avance para uma tutela penal eficaz e preventiva, fundamentada na cooperação internacional, na especialização técnica e na conscientização coletiva. Somente dessa forma será possível garantir a proteção integral dos direitos fundamentais na sociedade digital contemporânea.

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, representou um avanço relevante na tipificação de condutas ilícitas praticadas em ambiente digital. Contudo, sua abrangência ainda se mostra insuficiente diante da complexidade dos crimes cibernéticos modernos. A norma prevê punições apenas para a invasão de dispositivos informáticos com o intuito de obter, adulterar ou destruir dados, deixando de contemplar outras modalidades criminosas amplamente praticadas no ciberespaço, como phishing, ransomware, fraudes eletrônicas sem invasão direta e ataques de engenharia social. Conforme destaca Meirelles (2020), a legislação brasileira, embora pioneira no enfrentamento da criminalidade virtual, não acompanhou o ritmo da inovação tecnológica, criando lacunas que comprometem a efetividade da tutela penal no ambiente digital.

Essas limitações refletem-se especialmente na interpretação restritiva do tipo penal previsto no artigo 154-A do Código Penal, que exige invasão de dispositivo alheio sem autorização. De acordo com Dantas (2017) e Nascimento (2016), em situações em que o acesso é autorizado como em casos de compartilhamento de

senhas, dispositivos ou redes, não há configuração do crime, mesmo que os dados sejam posteriormente utilizados de maneira fraudulenta ou abusiva. Essa limitação impede o enquadramento penal de diversas condutas lesivas que ocorrem a partir de acessos inicialmente legítimos, mas que resultam em violações à privacidade e prejuízos patrimoniais e morais às vítimas.

Além disso, como aponta Furlan (2019), o avanço das tecnologias digitais e o surgimento constante de novas formas de ataque tornam indispensável a criação de tipos penais específicos que acompanhem a dinâmica do ambiente cibernético. O autor defende a necessidade de uma legislação mais detalhada, capaz de distinguir entre diferentes espécies de crimes digitais, como os que envolvem criptografia, mineração de dados, ataques a infraestruturas críticas e manipulação de algoritmos. Tal abordagem permitiria uma resposta penal mais justa e proporcional, evitando interpretações genéricas que possam gerar insegurança jurídica.

Outro ponto crítico é a dificuldade probatória que envolve os delitos informáticos. Segundo Carvalho (2023), a investigação e a persecução penal desses crimes enfrentam barreiras técnicas e institucionais, como a escassez de profissionais qualificados, a ausência de laboratórios forenses digitais em muitas regiões e a volatilidade das provas eletrônicas. O autor observa que, em razão dessas fragilidades, muitos casos são arquivados por falta de materialidade ou autoria comprovada, o que reduz o poder dissuasório da norma penal e alimenta o sentimento de impunidade entre os agentes criminosos.

A transnacionalidade dos delitos também acentua as limitações da Lei nº 12.737/2012. Como observa Meirelles (2020), grande parte das ações criminosas virtuais é praticada a partir de servidores localizados no exterior, o que dificulta a identificação e responsabilização dos autores. A ausência de tratados bilaterais e a morosidade dos mecanismos de cooperação internacional comprometem a eficácia das investigações e tornam o combate ao cibercrime ainda mais complexo.

Por outro lado, a autora ressalta que o Brasil vem tentando suprir essas lacunas por meio de iniciativas legislativas complementares, como a Lei nº 14.155/2021, que agravou as penas para delitos praticados por meios eletrônicos, e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que reforça a tutela da privacidade e da segurança da informação. No entanto, tais medidas ainda carecem de integração sistemática para garantir uma política pública eficaz de cibersegurança.

Em síntese, embora a Lei Carolina Dieckmann tenha representado um avanço histórico, ela permanece limitada em seu alcance e aplicação prática, exigindo atualização constante diante das transformações tecnológicas. Conforme apontam Dantas (2017), Furlan (2019) e Carvalho (2023), o futuro da tutela penal digital no Brasil depende de uma reformulação legislativa abrangente, aliada à capacitação técnica de profissionais e ao fortalecimento da cooperação internacional, de modo a assegurar a efetividade da proteção dos direitos fundamentais no ambiente digital.

4 EFETIVIDADE E DESAFIOS DA LEI CAROLINA DIECKMANN NA PROTEÇÃO PENAL CONTRA CRIMES CIBERNÉTICOS

A pesquisa revelou que a Lei nº 12.737/2012 (Lei Carolina Dieckmann) representou um importante marco jurídico na criminalização de condutas ilícitas praticadas no ambiente digital, inaugurando uma nova fase no Direito Penal brasileiro ao reconhecer a necessidade de tutelar penalmente a invasão de dispositivos informáticos e a violação da privacidade (Alcântara, 2022; Brasil, 2012). A análise demonstrou que essa norma foi fundamental para a consolidação da proteção de dados e da intimidade no ciberespaço, sendo considerada o ponto de partida para a construção do atual sistema normativo de segurança digital no país (Machado; Duarte, 2021).

Entretanto, observou-se que a eficácia prática da lei é limitada, já que a rápida evolução tecnológica produziu novas modalidades de criminalidade não contempladas pela norma, como fraudes eletrônicas, ataques de ransomware e crimes de engenharia social (Meirelles, 2020; Furlan, 2019). Essa defasagem legislativa evidencia a dificuldade do Estado em acompanhar a dinâmica dos delitos digitais, o que reduz a efetividade da resposta penal e amplia o espaço para a impunidade. Além disso, autores como Dantas (2017) e Nascimento (2016) destacam que, em situações de acesso autorizado como o uso indevido de senhas ou dispositivos compartilhados, o crime não se configura, revelando uma lacuna interpretativa que fragiliza a tutela penal.

A pesquisa bibliográfica também constatou um consenso entre os estudiosos quanto à necessidade de atualização contínua da legislação e de integração entre órgãos de investigação, bem como o fortalecimento da cooperação internacional para enfrentar a natureza transnacional dos crimes cibernéticos (Silva, 2020; Alexandre, 2023; Convenção de Budapeste, 2001). Para Meirelles (2020) e Guimarães (2024), o

enfrentamento do cibercrime deve envolver não apenas o aprimoramento jurídico, mas também o investimento em capacitação técnica e em políticas de alfabetização digital, de modo a prevenir a ocorrência de delitos antes mesmo de sua consumação.

Outro achado relevante foi a constatação de que o Brasil figura entre os países com maior número de ataques cibernéticos no mundo, conforme relatado pelo FortiGuard Labs (2022). Esse dado evidencia a fragilidade estrutural da segurança digital e reforça a urgência de políticas públicas voltadas à promoção de uma cultura de cibersegurança e educação digital (Bezerra, 2019; Castro, 2021). A vulnerabilidade das instituições públicas e privadas, aliada à falta de conscientização dos usuários, indica que o problema vai além da insuficiência penal, abrangendo aspectos sociais, educacionais e tecnológicos.

Em síntese, os resultados apontam que, embora a Lei Carolina Dieckmann tenha sido um marco no ordenamento jurídico brasileiro, seu alcance prático permanece restrito diante da complexidade dos crimes digitais contemporâneos. A efetividade dessa tutela penal depende de uma política integrada de prevenção, investigação e cooperação internacional, aliada à educação digital e à atualização legislativa constante, para que o Brasil possa enfrentar de forma eficiente os desafios da era digital e garantir a proteção dos direitos fundamentais no ciberespaço.

5 CONCLUSÃO

Conclui-se que a Lei nº 12.737/2012 (Lei Carolina Dieckmann) representou um marco inovador na criminalização das condutas ilícitas praticadas em ambiente digital, sendo o primeiro instrumento jurídico brasileiro voltado especificamente à repressão de crimes cibernéticos. Contudo, conforme indicam Alcântara (2022) e Meirelles (2020), o alcance dessa norma mostrou-se insuficiente diante da evolução tecnológica e da diversidade de delitos digitais contemporâneos, como fraudes eletrônicas, phishing e ataques de ransomware, que não se enquadram nas previsões originais da lei.

A hipótese da pesquisa foi confirmada, uma vez que se constatou que o ordenamento jurídico brasileiro ainda carece de mecanismos modernos e eficazes para a prevenção e repressão das condutas criminosas praticadas no ciberespaço. Autores como Dantas (2017) e Furlan (2019) ressaltam que a legislação vigente precisa acompanhar o ritmo acelerado das inovações tecnológicas, de modo a garantir uma tutela penal adequada às novas formas de violação de privacidade e segurança informacional.

O estudo também evidencia a necessidade de revisões legislativas periódicas, maior investimento em tecnologia investigativa e fortalecimento da cooperação internacional, conforme destacam Silva (2020) e Alexandre (2023). Esses elementos são essenciais para enfrentar a natureza transnacional dos crimes cibernéticos, que ultrapassam fronteiras físicas e desafiam os mecanismos tradicionais de persecução penal.

No entanto, os resultados da pesquisa demonstram que a norma possui limitações significativas, como a ausência de previsão para crimes digitais mais sofisticados, como phishing, ransomware e fraudes eletrônicas sem invasão direta. Entre as principais contribuições do estudo, destaca-se a necessidade de integração normativa com o Marco Civil da Internet e a Lei Geral de Proteção de Dados, bem como o fortalecimento da investigação digital e da cooperação internacional.

Por fim, reforça-se que a efetiva proteção da privacidade e da segurança da informação não depende apenas da criação de novas leis, mas de um esforço conjunto que envolva educação digital, conscientização social e capacitação estatal. Como defendem Guimarães (2024) e Bezerra (2019), somente por meio da formação de uma cultura sólida de cibersegurança será possível garantir que o Direito Penal cumpra seu papel de proteção dos direitos fundamentais na era da informação.

Recomenda-se, portanto, a formulação de políticas públicas que aliem repressão penal, educação digital e conscientização social, visando à construção de um ambiente virtual mais seguro e à proteção efetiva dos direitos fundamentais na era da informação.

REFERÊNCIAS

- ALCANTARA, Gabriella Souza de. Os crimes cibernéticos e a ineficácia da Lei Carolina Dieckmann no âmbito do Direito Penal. 2022. 59 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2022. Disponível em: <https://pantheon.ufrj.br/handle/11422/22846>. Acesso em: 11.out.2025.
- ARRUDA, Vanessa Cristina Dias; LIMA, Marília Freitas. Crimes cibernéticos: análise da legislação civil e penal vigente no Brasil. *RECIMA21 – Revista Científica Multidisciplinar*, v. 4, n. 12, 2023. Disponível em: <https://doi.org/10.47820/recima21.v4i12.4578>. Acesso em: 20.set.2025
- BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 set.2025.
- BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 24 set.2025
- BOULAY, Benedict du. *Inteligência Artificial na Educação e Ética*. RE@D - Revista de Educação a Distância e Elearning, v. 6, n. 1, p. 1–17, jan./jun. 2023. Disponível em: https://doi.org/10.1007/978-981-19-0351-9_6-2. Acesso em: 24 out. 2025.
- BOBBIO, Norberto. *A era dos direitos*. 9. ed. Rio de Janeiro: Elsevier, 1992. Disponível em: https://www.mprj.mp.br/documents/20184/172905/a_era_dos_direitos.pdf. Acesso em: 12 de out.2025
- CASTELLS, Manuel. *A sociedade em rede*. 17. ed. São Paulo: Paz e Terra, 2021. Disponível em: <https://globalizacaoeintegracaoaregionalufabc.wordpress.com/wpcontent/uploads/2014/10/castells-m-a-sociedade-em-rede.pdf> Acesso em: 22.ago.2025.
- CITRON, D. K.; PASQUALE, F. A. *A sociedade pontuada: devido processo para previsões automatizadas*. *Washington Law Review*, v. 89, n. 1, p. 1-34, 2014. Disponível em: <https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2>. Acesso em: 14.out.2025.
- CRAWFORD, Kate. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven: Yale University Press, 2021. Disponível em: [10.56315/PSCF3-22Crawford](https://doi.org/10.56315/PSCF3-22Crawford). Acesso em: 25.out.2025;

DONEDA, Danilo. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Revista dos Tribunais, 2022. Disponível em: <https://repositorio.ufba.br/bitstream/ri/35799/3/protecao-de-dados-pessoais-RI.pdf>. Acesso em: 14.set.2025.

DONEDA, Danilo. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Revista dos Tribunais, 2022. Disponível em: <https://repositorio.ufba.br/bitstream/ri/35799/3/protecao-de-dados-pessoais-RI.pdf>. Acesso em: 14.set.2025.

EUROPEAN PARLIAMENT. *Artificial Intelligence Act: EU rules to ensure AI is safe and respects fundamental rights*. Brussels: European Parliament, 2023. Disponível em: <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-actfirst-regulation-on-artificial-intelligence>. Acesso em: 10.out.2025

EUROPEAN UNION. *General Data Protection Regulation (GDPR)*. Official Journal of the European Union, Brussels, 2018. Disponível em: <https://eurlex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 10.out.2025.

FALANGOLA, Renata de Farias et al. *A regulação da inteligência artificial no Brasil: desafios jurídicos, éticos e sociais*. *Revista Científica Multidisciplinar Lattice*, v. 2, n. 4, p. 1–23, 2025. Disponível em: <https://doi.org/10.70579/pl.v2i4.96>. Acesso em: 28.out.2025

FERRAJOLI, Luigi. *Poderes selvagens: a crise da democracia constitucional*. São Paulo: Editora Unesp, 2019. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:redes.virtual.bibliotecas:livro:2014;001010983>. Acesso em: 17.set.2025.

FLORIDI, Luciano. *The Logic of Information: A Theory of Philosophy as Conceptual Design*. Oxford: Oxford University Press, 2019.

FLORIDI, Luciano; COWLS, Josh. *A unified framework of five principles for AI in society*. *Harvard Data Science Review*, v. 1, n. 1, p. 1–13, 2019. Disponível em: <https://doi.org/10.1162/99608f92.8cd550d1>. Acesso em: 24 out. 2025.

G1. *Advogado usa casos inventados pelo ChatGPT em processo judicial e leva puxão de orelha de juiz*. 29 maio 2023. Disponível em: <https://g1.globo.com/tecnologia/noticia/2023/05/29/advogado-usa-casos-inventados-pelo-chatgpt-em-processo-judicial-e-leva-puxao-de-orelha-de-juiz.ghtml>. Acesso em: 08 out. 2024.

JONAS, Hans. *O princípio responsabilidade: ensaio de uma ética para a civilização tecnológica*. Rio de Janeiro: Contraponto, 2006. Disponível em: ... Acesso em:

JUSBRASIL. *Inteligência artificial vai agilizar a tramitação de processos no STF*. 21 mar. 2018. Disponível em: <https://www.jusbrasil.com.br/noticias/inteligencia-artificialvai-agilizar-a-tramitacao-de-processos-no-stf/584499448>. Acesso em: 04 nov. 2024.

LEAVITT, David. *O homem que sabia demais: Alan Turing e a invenção do computador*. São Paulo: Novo Conceito, 2007. Disponível em: <https://books.google.com/books>. Acesso em: 05.out.2025

MITTELSTADT, Brent D. et al. *The ethics of algorithms: Mapping the debate*. *Big Data & Society*, v. 3, n. 2, p. 1–21, 2016. Disponível em: <https://journals.sagepub.com/doi/10.1177/2053951716679679>. Acesso em: 11.out.2025.

MCCARTHY, John. *What is Artificial Intelligence?* Stanford Encyclopedia of Philosophy, 2007. Disponível em: https://cicerocq.wordpress.com/wpcontent/uploads/2018/08/trabalho1_ia_dinter_ufrgs_ufma_uema_cicero.pdf. Acesso em: 23.out.2025.

NUNES, Dierle; RUBINGER, Paula Caetano; MARQUES, Ana Luiza. *Os perigos do uso da inteligência artificial na advocacia*. 9 jul. 2018. Disponível em: <https://www.conjur.com.br/2018-jul-09/opinioao-perigos-uso-inteligencia-artificialadvocacia/>. Acesso em: 14.out.2025.

OLIVEIRA, Ana. *O impacto da inteligência artificial na pesquisa jurídica*. *Revista Brasileira de Direito Digital*, 2020. Disponível em: <https://doi.org/10.61164/rjnm.v7i1.2010> Acesso em: 10.out.2025.

OECD. *OECD Principles on Artificial Intelligence*. Paris: Organisation for Economic Co-operation and Development, 2019. Disponível em: <https://www.oecd.org/en/topics/aiprinciples.html#:~:text=The%20OECD%20AI%20Principles%20promote,stand%20th e%20test%20of%20time>. Acesso em: 10.out.2025.

OLIVEIRA, Daniel Calegar. *Direitos fundamentais e a era digital: limites no exercício dos direitos fundamentais e sua aplicação na internet*. Manhauçu: UNIFACIG, 2023. Disponível em: <https://pensaracademico.unifacig.edu.br/index.php/repositorioctcc/article/view/4164/3179>. Acesso em: 16.out.2025.

PERFILADV: *1º estudo demográfico da advocacia brasileira*. Coord. José Alberto Simonetti; Rafael de Assis Horn; Luis Felipe Salomão. Brasília; Rio de Janeiro: OAB Nacional; FGV Justiça, 2024. Disponível em:

https://conhecimento.fgv.br/sites/default/files/2025-01/publicacoes/perfil_adv_1oestudo_demografico_da_advocacia_brasileira.pdf. Acesso em: 18.out.2025.

QUEIROZ, Aíla Marques de; BUENO, Pedro Lucas Nogueira; LISBINO, Jhon Kennedy Teixeira. *O impacto da inteligência artificial na advocacia brasileira: benefícios e desafios no setor jurídico*. Revista Ibero-Americana de Humanidades, Ciências e Educação, São Paulo, v. 10, n. 11, nov. 2024. doi:10.51891/rease.v10i11.16691.

SALDANHA, Júlia. *Tecnologia e desigualdade: os desafios da inclusão digital no Brasil*. Rio de Janeiro: FGV Editora, 2023. Disponível em: <https://periodicorease.pro.br/rease/article/view/16691>. Acesso em: 02.out.2025.

SARLET, Ingo Wolfgang. *Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988*. 13. ed. Porto Alegre: Livraria do Advogado, 2020. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:redes.virtual.bibliotecas:livro:2019;001190467>. Acesso em: 09.out.2025.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 47. ed. São Paulo: Malheiros, 2022. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:redes.virtual.bibliotecas:livro:2018;001116292>. Acesso em: 09.out.2025.

SUSSKIND, Richard; SUSSKIND, Daniel. *O futuro das profissões: como a tecnologia transformará o trabalho dos especialistas humanos*. Oxford University Press, 2018. TJPI. *JuLIA: inteligência artificial do TJ-PI é apresentada durante congresso de inovação do Poder Judiciário*. 2024. Disponível em: <https://www.tjpi.jus.br/portaltjpi/tjpi/noticias-tjpi/julia-inteligencia-artificial-do-tj-pi-eapresentada-durante-congresso-de-inovacao-do-poder-judiciario/>. Acesso em: 08.set. 2025.

UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. Paris: United Nations Educational, Scientific and Cultural Organization, 2021. Disponível em: <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence>. Acesso em: 17.out.2025.

WILLIAMSON, Ben. *Silicon startup schools: Technocracy, algorithmic imaginaries and venture philanthropy in corporate education reform*. *Critical Studies in Education*, v. 59, p. 218–236, 2018. Disponível em: <https://doi.org/10.1080/17508487.2016.1186710>. Acesso em: 24 out. 2025.

ZANATTA, Rafael A. *Direito e inteligência artificial: perspectivas para a governança algorítmica*. *Revista Direito GV*, v. 17, n. 2, p. 1–30, 2021. Disponível em: <https://doi.org/10.11606/issn.2316-9036.i141p51-64> Acesso em: 10.out.2025.

ZEIDE, Elana. *Artificial Intelligence in Higher Education: Applications, Promise and Perils, and Ethical Questions*. *Educause Review*, p. 31–39, 2019. Disponível em: <https://er.educause.edu/-/media/files/articles/2019/8/er193104.pdf>. Acesso em: 24 out. 2025.