RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

O Direito à Privacidade na Era Digital: Uma Análise da Lei Carolina Dieckmann

The Right to Privacy in the Digital Age: An Analysis of the Carolina Dieckmann Law
El Derecho a la Privacidad en la Era Digital: Un Análisis de la Ley Carolina Dieckmann

Regina Barboza Lima – Faculdade Católica de Rondônia (FCR), Porto Velho-RO, Regina.lima@sou.fcr.edu.br
Ana Cláudia Miranda Lopes Assis – Faculdade Católica de Rondônia (FCR), ana.assis@fcr.edu.br

Resumo:
O presente artigo analisa o direito à privacidade na era digital a partir da Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, examinando sua importância, seus limites e sua articulação com o sistema brasileiro de proteção da intimidade, da vida privada e dos dados pessoais. A pesquisa parte do seguinte problema: em que medida a Lei Carolina Dieckmann é eficaz para proteger a privacidade no ambiente digital diante da evolução tecnológica, das novas formas de criminalidade cibernética e da ampliação constitucional do direito à proteção de dados pessoais? Como hipótese, sustenta-se que a referida lei representou marco indispensável para a tutela penal da privacidade digital, ao tipificar a invasão de dispositivo informático, mas sua suficiência é relativa, pois a proteção da pessoa no ciberespaço exige interpretação integrada com a Constituição Federal, o Código Civil, o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e legislações posteriores, como a Lei n.º 14.132/2021, que tipificou o crime de perseguição. O objetivo geral consiste em avaliar a eficácia da Lei Carolina Dieckmann na proteção da privacidade digital. Como objetivos específicos, busca-se: compreender a evolução do conceito de privacidade para a noção de autodeterminação informativa; analisar o crime de invasão de dispositivo informático previsto no art. 154-A do Código Penal; distinguir a proteção penal da privacidade das tutelas civil, constitucional e administrativa; e examinar os desafios decorrentes de práticas como phishing, roubo de dados, exposição indevida de informações pessoais e ciberstalking. A metodologia adotada é bibliográfica e documental, com abordagem qualitativa, fundada na análise da legislação, da doutrina e do contexto normativo relacionado aos crimes cibernéticos e à proteção de dados pessoais. Conclui-se que a Lei Carolina Dieckmann permanece relevante como ponto de partida da tutela penal da privacidade digital, especialmente após as alterações promovidas pela Lei n.º 14.155/2021, que reforçaram a resposta penal à invasão de dispositivo informático. Todavia, sua efetividade depende de uma compreensão sistêmica e articulada, capaz de combinar repressão penal, prevenção, educação digital, segurança da informação, responsabilização civil e proteção de dados pessoais.

Palavras-chave:
Ciberstalking. Crimes cibernéticos. Direito à privacidade. Lei Carolina Dieckmann. Proteção de Dados Pessoais.

Abstract:
This article analyzes the right to privacy in the digital age based on Law No. 12.737/2012, known as the Carolina Dieckmann Law, examining its importance, its limits, and its articulation with the Brazilian system for the protection of intimacy, private life, and personal data. The research starts from the following problem: to what extent is the Carolina Dieckmann Law effective in protecting privacy in the digital environment in the face of technological evolution, new forms of cybercrime, and the constitutional expansion of the right to the protection of personal data? As a hypothesis, it is argued that the aforementioned law represented an indispensable milestone for the criminal protection of digital privacy, by criminalizing the

invasion of computer devices, but its sufficiency is relative, since the protection of the person in cyberspace requires integrated interpretation with the Federal Constitution, the Civil Code, the Marco Civil da Internet (Brazilian Internet Bill of Rights), the General Law on the Protection of Personal Data, and subsequent legislation, such as Law No. 14.132/2021, which criminalized stalking. The overall objective is to evaluate the effectiveness of the Carolina Dieckmann Law in protecting digital privacy. Specific objectives include: understanding the evolution of the concept of privacy towards the notion of informational self-determination; analyzing the crime of unauthorized access to computer devices as defined in Article 154-A of the Penal Code; distinguishing the criminal protection of privacy from civil, constitutional, and administrative protections; and examining the challenges arising from practices such as phishing, data theft, improper disclosure of personal information, and cyberstalking. The methodology adopted is bibliographic and documentary, with a qualitative approach, based on the analysis of legislation, doctrine, and the normative context related to cybercrimes and the protection of personal data. It is concluded that the Carolina Dieckmann Law remains relevant as a starting point for the criminal protection of digital privacy, especially after the amendments introduced by Law No. 14.155/2021, which reinforced the criminal response to unauthorized access to computer devices. However, its effectiveness depends on a systemic and articulated understanding, capable of combining criminal repression, prevention, digital education, information security, civil liability, and personal data protection.

Keywords:
Digital crimes. Right to privacy. General Data Protection Law. Civil Framework for the Internet.

Resumen:
El presente artículo analiza el derecho a la privacidad en la era digital a partir de la Ley n.º 12.737/2012, conocida como Ley Carolina Dieckmann, examinando su importancia, sus límites y su articulación con el sistema brasileño de protección de la intimidad, la vida privada y los datos personales. La investigación parte del siguiente problema: ¿en qué medida la Ley Carolina Dieckmann es eficaz para proteger la privacidad en el entorno digital frente a la evolución tecnológica, las nuevas formas de ciberdelincuencia y la ampliación constitucional del derecho a la protección de datos personales? Como hipótesis, se sostiene que dicha ley representó un hito indispensable para la tutela penal de la privacidad digital al tipificar la invasión de dispositivos informáticos; sin embargo, su suficiencia es relativa, ya que la protección de la persona en el ciberespacio exige una interpretación integrada con la Constitución Federal, el Código Civil, el Marco Civil de Internet, la Ley General de Protección de Datos Personales y legislaciones posteriores, como la Ley n.º 14.132/2021, que tipificó el delito de acoso. El objetivo general consiste en evaluar la eficacia de la Ley Carolina Dieckmann en la protección de la privacidad digital. Como objetivos específicos, se busca comprender la evolución del concepto de privacidad hacia la noción de autodeterminación informativa; analizar el delito de invasión de dispositivo informático previsto en el artículo 154-A del Código Penal; distinguir la protección penal de la privacidad de las tutelas civil, constitucional y administrativa; y examinar los desafíos derivados de prácticas como el phishing, el robo de datos, la divulgación indebida de información personal y el ciberacoso. La metodología adoptada es bibliográfica y documental, con enfoque cualitativo, fundamentada en el análisis de la legislación, la doctrina y el contexto normativo relacionado con los delitos cibernéticos y la protección de datos personales. Se concluye que la Ley Carolina Dieckmann sigue siendo relevante como punto de partida para la tutela penal de la privacidad digital, especialmente después de las modificaciones introducidas por la Ley n.º 14.155/2021, que reforzaron la respuesta penal frente a la invasión de dispositivos informáticos. No obstante, su efectividad depende de una comprensión

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

sistémica y articulada, capaz de combinar represión penal, prevención, educación digital, seguridad de la información, responsabilidad civil y protección de datos personales.

Palabras clave:
Ciberacoso. Delitos cibernéticos. Derecho a la privacidad. Ley Carolina Dieckmann. Protección de datos personales.

1 Introdução

As relações sociais contemporâneas foram profundamente transformadas pelo avanço das tecnologias de informação e comunicação. Atividades antes restritas ao espaço físico passaram a ocorrer em ambientes digitais, como redes sociais, aplicativos de mensagens, plataformas de armazenamento, sistemas bancários, serviços públicos eletrônicos e dispositivos informáticos conectados à internet. Essa nova realidade ampliou as possibilidades de comunicação, acesso à informação e participação social, mas também intensificou os riscos de violação à intimidade, à vida privada, à honra, à imagem e aos dados pessoais[1].

Nesse cenário, o direito à privacidade, assegurado pela Constituição Federal de 1988, passou a enfrentar desafios próprios da sociedade digital. A vida privada deixou de estar concentrada apenas em espaços físicos ou documentos materiais e passou a ser projetada em celulares, computadores, contas digitais, bancos de dados, plataformas online e sistemas de comunicação em rede. Com isso, invasões de dispositivos, acessos indevidos, exposição de imagens, divulgação não autorizada de informações pessoais, phishing, roubo de credenciais, fraudes digitais e práticas de perseguição virtual passaram a representar ameaças concretas à dignidade da pessoa humana.

Historicamente, o ordenamento jurídico brasileiro encontrava dificuldades para enquadrar penalmente determinadas condutas praticadas no ambiente informático. Antes da Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, a invasão de dispositivos e a obtenção indevida de arquivos digitais eram frequentemente analisadas a partir de tipos penais tradicionais, nem sempre adequados à natureza dos dados e informações armazenados em meio eletrônico. Essa dificuldade gerava insegurança jurídica, especialmente porque os dados

[1] COPETTI, Rafael; MIRANDA, Marcel Andreata De.et al. **Autodeterminação Informativa e Proteção de Dados: Uma Análise Crítica da Jurisprudência Brasileira. Direito, governança e novas tecnologias**. Florianópolis: CONPEDI, 2015. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/j6023guzncw4in57.pdf> Acesso em: 10 jun. 2026.

digitais podem ser copiados, reproduzidos ou compartilhados sem que haja, necessariamente, subtração física do bem.

A Lei n.º 12.737/2012 surgiu, portanto, como resposta legislativa relevante a uma lacuna específica do Direito Penal brasileiro, ao introduzir no Código Penal o crime de invasão de dispositivo informático. Sua edição foi impulsionada por caso de grande repercussão pública envolvendo a exposição indevida da intimidade de pessoa conhecida nacionalmente, o que evidenciou a necessidade de proteção penal mais adequada contra acessos não autorizados a dispositivos e informações pessoais.

Apesar de sua importância histórica, a Lei Carolina Dieckmann não pode ser analisada de forma isolada. A evolução tecnológica, o surgimento de novas formas de criminalidade digital e a ampliação do sistema normativo de proteção da privacidade exigem uma interpretação integrada. A Constituição Federal protege a intimidade, a vida privada, a honra e a imagem; a Emenda Constitucional n.º 115/2022 incluiu a proteção de dados pessoais como direito fundamental autônomo; o Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet; a Lei Geral de Proteção de Dados Pessoais disciplina o tratamento de dados pessoais; e o Código Penal passou por novas atualizações, como a Lei n.º 14.155/2021, que alterou o art. 154-A, e a Lei n.º 14.132/2021, que tipificou o crime de perseguição.

Diante desse contexto, o problema central da presente pesquisa consiste em investigar em que medida a Lei n.º 12.737/2012 é eficaz para proteger a privacidade na era digital, considerando as alterações legislativas posteriores, a autonomia constitucional da proteção de dados pessoais e a complexidade técnica dos crimes cibernéticos. A hipótese adotada é a de que a Lei Carolina Dieckmann representou marco indispensável para a tutela penal da privacidade digital, mas sua suficiência é relativa, pois a proteção efetiva da pessoa no ambiente virtual depende da articulação entre repressão penal, tutela civil, proteção constitucional, segurança da informação, educação digital e regime jurídico de proteção de dados pessoais.

O objetivo geral do estudo é avaliar a eficácia da Lei Carolina Dieckmann na proteção da privacidade digital. Como objetivos específicos, busca-se: compreender a evolução do conceito de privacidade para a noção de autodeterminação informativa; analisar o crime de invasão de dispositivo informático previsto no art. 154-A do Código Penal; examinar as alterações promovidas pela Lei n.º 14.155/2021; distinguir a proteção penal da privacidade das tutelas civil, constitucional e administrativa; e relacionar a Lei Carolina Dieckmann com outros instrumentos normativos relevantes, como o Marco Civil da Internet, a LGPD e a Lei do Stalking.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

A metodologia adotada é de natureza bibliográfica e documental, com abordagem qualitativa. A pesquisa fundamenta-se na análise da legislação brasileira, da doutrina especializada e de normas relacionadas à proteção da privacidade, dos dados pessoais e ao enfrentamento dos crimes cibernéticos. O estudo parte de uma perspectiva jurídico-dogmática, buscando compreender os limites e as possibilidades da tutela penal da privacidade no ambiente digital, sem desconsiderar a necessária articulação com os demais mecanismos de proteção da pessoa.

A relevância da pesquisa justifica-se pela crescente exposição dos indivíduos a riscos digitais e pela necessidade de compreender como o Direito pode responder às novas formas de violação da intimidade e dos dados pessoais. A análise da Lei Carolina Dieckmann permite verificar os avanços promovidos pelo legislador brasileiro, mas também evidencia que a proteção da privacidade na era digital não depende apenas da punição posterior à invasão de dispositivos. Exige-se, também, prevenção, educação digital, segurança da informação, responsabilização civil e administrativa, cooperação institucional e fortalecimento da cultura de proteção de dados pessoais.

Além da invasão de dispositivos informáticos, a pesquisa também aborda práticas como o ciberstalking e a exposição indevida de informações pessoais, pois tais condutas demonstram que a privacidade digital pode ser violada tanto pelo acesso não autorizado a dados armazenados quanto pela perseguição reiterada, vigilância abusiva, ameaça de divulgação de informações e perturbação da liberdade da vítima no ambiente virtual. Essa ampliação do debate é essencial para compreender que a tutela jurídica contemporânea não deve se limitar à proteção do equipamento eletrônico, mas deve alcançar a pessoa, sua intimidade, sua autonomia, sua liberdade, sua integridade psicológica e sua autodeterminação informativa.

Dessa forma, o presente trabalho busca demonstrar que a Lei Carolina Dieckmann permanece relevante para a proteção penal da privacidade digital, mas deve ser compreendida como parte de um ecossistema normativo mais amplo. A efetividade da proteção da pessoa na era digital depende da interação entre Constituição Federal, Código Civil, Marco Civil da Internet, LGPD, Código Penal e legislações específicas voltadas ao enfrentamento das novas formas de violação da intimidade, da vida privada e dos dados pessoais.

2 Referencial teórico

2.1 Privacidade, intimidade e proteção de dados pessoais na sociedade digital

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

A proteção da privacidade e da intimidade constitui direito fundamental assegurado pela Constituição Federal de 1988, especialmente no art. 5º, inciso X, que reconhece a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurando indenização pelo dano material ou moral decorrente de sua violação. No ambiente digital, essa proteção assume especial relevância, pois a vida privada passou a ser projetada em dispositivos informáticos, redes sociais, aplicativos de mensagens, plataformas digitais, bancos de dados e sistemas de comunicação em rede.

Tradicionalmente, o direito à privacidade foi compreendido a partir de uma concepção negativa, associada ao "direito de ser deixado só", isto é, à proteção do indivíduo contra intromissões indevidas em sua esfera privada. Todavia, essa compreensão tornou-se insuficiente diante da sociedade informacional e do avanço das tecnologias de informação e comunicação.[2]

No cenário digital, a privacidade passou a envolver também uma dimensão ativa de controle sobre informações pessoais, compreendendo a possibilidade de o indivíduo influenciar o acesso, a exposição, o compartilhamento, a finalidade e o uso de dados relacionados à sua vida pessoal.

Essa evolução conduz à noção de autodeterminação informativa, compreendida como o direito de a pessoa exercer controle sobre seus próprios dados e informações pessoais, acompanhando e influenciando a forma como são coletados, utilizados, armazenados, compartilhados e eliminados.[3] Assim, o titular deixa de ser apenas alguém protegido contra invasões indevidas e passa a ser reconhecido como sujeito ativo no controle da circulação de suas informações.

Nesse contexto, é necessário distinguir privacidade e proteção de dados pessoais. A privacidade protege a esfera íntima, a vida privada e a reserva pessoal do indivíduo contra exposições, interferências ou intromissões indevidas. A proteção de dados pessoais, por sua vez, alcança qualquer informação relacionada a pessoa natural identificada ou identificável, ainda que essa informação não seja, em si, íntima ou sensível. Dados como nome, CPF,

---

[2] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Ver também: COOLEY, Thomas McIntyre. **A treatise on the law of torts, or the wrongs which arise independent of contract**. Chicago: Callaghan and Company, 1879; WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890.

[3] MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. *Migalhas*, 30 out. 2020; DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

localização, endereço eletrônico, registros de acesso, hábitos de navegação e perfil de consumo podem não revelar diretamente a intimidade da pessoa, mas seu tratamento inadequado pode afetar sua liberdade, autonomia, dignidade e autodeterminação informativa.

A Emenda Constitucional n.º 115/2022 consolidou essa evolução ao incluir no art. 5º, inciso LXXIX, da Constituição Federal, o direito fundamental à proteção dos dados pessoais, inclusive nos meios digitais.[4] Com isso, a proteção de dados passou a figurar expressamente no catálogo de direitos fundamentais, sem se confundir com a privacidade, embora historicamente conectada a ela.

Desse modo, no ambiente virtual, a proteção da privacidade, da intimidade e dos dados pessoais revela-se indispensável para a preservação da liberdade e da dignidade humana. A exposição indevida de informações, a invasão de dispositivos, o uso abusivo de dados e a ausência de transparência no tratamento de informações pessoais podem comprometer não apenas a esfera privada do indivíduo, mas também sua autonomia, sua segurança, sua reputação e sua capacidade de participação livre na vida social.[5]

2.2 Tutela civil-constitucional da privacidade digital

A proteção da privacidade no Brasil possui fundamento civil-constitucional. Isso significa que a privacidade não deve ser compreendida apenas como interesse individual disponível ou como simples relação entre particulares, mas como direito fundamental vinculado à dignidade da pessoa humana, à liberdade, à intimidade e ao livre desenvolvimento da personalidade.

No plano constitucional, o art. 5º, inciso X, da Constituição Federal assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem. O inciso XII do mesmo artigo também protege o sigilo da correspondência e das comunicações telegráficas, de dados e telefônicas, ressalvadas as hipóteses legais e mediante ordem judicial, quando cabível. Esses dispositivos formam a base constitucional da proteção da vida privada também no ambiente digital.

---

[4] BRASIL. **Emenda Constitucional n.º 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais.

[5] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008; BIONI, Bruno Ricardo. **Regulação e Proteção de Dados Pessoais: o princípio da accountability**. Rio de Janeiro: Forense, 2022.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

No plano civil, o Código Civil concretiza essa tutela por meio dos direitos da personalidade, estabelecendo o art. 21 que a vida privada da pessoa natural é inviolável, autorizando o juiz, a requerimento do interessado, a adotar providências necessárias para impedir ou fazer cessar ato contrário a essa norma. O art. 187 considera ilícito o exercício abusivo de um direito, especialmente quando o titular excede os limites impostos pela boa-fé, pelos bons costumes ou pela finalidade econômica e social do direito.

Assim, a invasão de dispositivo informático, o acesso indevido a contas pessoais, a divulgação não autorizada de imagens, o compartilhamento abusivo de informações privadas e o uso irregular de dados pessoais podem configurar não apenas ilícitos penais, mas também ilícitos civis. No campo penal, exige-se tipicidade estrita; no campo civil, a proteção é mais ampla, pois busca impedir, cessar ou reparar violações aos direitos da personalidade.

Essa compreensão é relevante para a presente pesquisa porque demonstra que a Lei Carolina Dieckmann não atua isoladamente. Ela integra um sistema mais amplo de tutela da pessoa na era digital, composto pela Constituição Federal, pelo Código Civil, pelo Marco Civil da Internet, pela LGPD e pelas normas penais específicas voltadas ao enfrentamento de condutas praticadas no ambiente virtual.

2.3 Marco normativo da proteção da privacidade no ambiente digital

O Marco Civil da Internet, Lei n.º 12.965/2014, representa importante marco normativo para a disciplina do uso da internet no Brasil. Sua relevância decorre do fato de estabelecer princípios, garantias, direitos e deveres aplicáveis ao ambiente digital, funcionando como matriz normativa voltada à organização jurídica das relações desenvolvidas na rede.

Trata-se de legislação de natureza predominantemente principiológica, voltada à fixação de parâmetros gerais para o uso da internet no país. O art. 3º do Marco Civil da Internet estabelece, entre seus princípios, a garantia da liberdade de expressão, comunicação e manifestação do pensamento, a proteção da privacidade, a proteção dos dados pessoais “na forma da lei”, a preservação e garantia da neutralidade de rede, a estabilidade, segurança e funcionalidade da rede, bem como a responsabilização dos agentes conforme suas atividades.

Por essa razão, o Marco Civil da Internet não deve ser tratado como regime geral de proteção de dados pessoais. Ele antecipa e estrutura princípios essenciais para a tutela dos direitos dos usuários na internet, criando uma base normativa posteriormente densificada pela LGPD. Nesse sentido, pode ser compreendido como uma espécie de “Constituição da Internet”,

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

por estabelecer fundamentos e diretrizes gerais para o ambiente digital, sem substituir a disciplina técnica e específica da proteção de dados pessoais.[6]

A Lei Geral de Proteção de Dados Pessoais, Lei n.º 13.709/2018, por sua vez, representa o principal regime jurídico brasileiro voltado à disciplina do tratamento de dados pessoais. Sua finalidade é proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural, estabelecendo regras aplicáveis às operações de tratamento realizadas por pessoas naturais ou jurídicas, de direito público ou privado, em meios físicos ou digitais.[12]

A LGPD não possui natureza penal nem deve ser compreendida como lei genérica de privacidade. Trata-se de norma técnica, principiológica e procedimental, voltada à regulação das atividades de coleta, armazenamento, utilização, compartilhamento, eliminação e demais formas de tratamento de dados pessoais. Enquanto a Lei Carolina Dieckmann atua no campo penal, ao tipificar a invasão de dispositivo informático, a LGPD atua em dimensão preventiva, regulatória, administrativa e civil, disciplinando a forma como os dados pessoais devem ser tratados de modo lícito, transparente, seguro e responsável.[7]

Entre os princípios da LGPD, destacam-se finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. A lei também assegura ao titular direitos como confirmação da existência de tratamento, acesso, correção, anonimização, bloqueio, eliminação, portabilidade, informação sobre compartilhamento, revogação do consentimento e oposição a tratamentos irregulares.[1]

Portanto, o Marco Civil da Internet e a LGPD exercem funções distintas e complementares. O primeiro estrutura princípios gerais para o uso da internet; a segunda disciplina tecnicamente o tratamento de dados pessoais. Ambos, contudo, integram o mesmo ecossistema normativo de proteção da pessoa no ambiente digital.

---

[6] ASSIS, Ana Cláudia Miranda Lopes. **Compliance digital e a proteção de dados no ensino fundamental: uma análise sob a ótica da LGPD acerca dos desafios e das perspectivas para a educação pública do município de Porto Velho–RO**. 2024. Tese (Doutorado em Direito) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2024. Disponível em: Disponível em: https://tede2.pucrs.br/tede2/handle/tede/12012. Acesso em: 14 mai. 2026.

[7] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**, arts. 1º, 5º, 6º, 7º, 18, 42 e 46; PECK, Patrícia Pinheiro. **Proteção de Dados Pessoais: comentários à Lei n.º 13.709/2018 (LGPD)**. 4. ed. São Paulo: SaraivaJur, 2023.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

2.4 Crimes cibernéticos e proteção penal da privacidade

A evolução tecnológica modificou profundamente as formas de interação social, econômica e comunicacional, mas também ampliou os riscos de violação a direitos fundamentais. A internet e os dispositivos informáticos passaram a ser utilizados não apenas como instrumentos de comunicação e acesso à informação, mas também como meios para a prática de condutas ilícitas que atingem a privacidade, o patrimônio, a honra, a liberdade e a segurança dos indivíduos.

Os crimes cibernéticos podem ser compreendidos como condutas penalmente relevantes praticadas mediante o uso de computadores, redes de computadores, dispositivos eletrônicos, sistemas informáticos ou ambientes digitais. Esses meios podem funcionar como instrumento para a prática do delito ou constituir o próprio objeto da conduta criminosa.[8]

A doutrina costuma distinguir os crimes cibernéticos próprios e impróprios, sendo os primeiros aquele em que o ambiente digital, os sistemas informáticos ou os dados eletrônicos integram a própria estrutura do delito, como ocorre na invasão de dispositivo informático. Já os crimes cibernéticos impróprios correspondem a delitos tradicionais praticados por meio da internet ou de tecnologias digitais, como estelionato, ameaça, difamação, divulgação indevida de imagens e outras condutas que poderiam ocorrer fora do ambiente virtual, mas que são potencializadas pela tecnologia.[9]

A criminalidade digital apresenta desafios específicos, como a velocidade de execução das condutas, a rápida disseminação de informações, a dificuldade de identificação dos autores, a volatilidade das provas digitais, a transnacionalidade de determinadas práticas e a necessidade de perícia especializada. Tais elementos demonstram que o enfrentamento dos crimes cibernéticos exige não apenas repressão penal, mas também prevenção, educação digital, segurança da informação, cooperação institucional e atualização legislativa constante.[10]

---

[8] COLLI, Maciel. **Cibercrimes: limites e perspectivas à investigação policial de crimes cibernéticos**. Curitiba: Juruá, 2010; ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

[9] WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. 2. ed. Rio de Janeiro: Brasport, 2013; ROSA, Fabrizio Rosa. **Crimes cibernéticos: aspectos penais e processuais**. São Paulo: JH Mizuno, 2017.

[10] MARCELI, Vilma Maria; DAHER, Roberto José. **Análise evolutiva dos crimes cibernéticos e a legislação penal brasileira**. *Revista Eletrônica FACP*, ano XV, n. 28, p. 100-116, mar. 2026.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

2.5 A Lei Carolina Dieckmann e a invasão de dispositivo informático

A Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, representa marco relevante na evolução da tutela penal da privacidade digital no Brasil. Sua edição ocorreu em contexto de crescente exposição das pessoas a riscos decorrentes do uso de computadores, celulares, redes sociais, aplicativos e demais dispositivos informáticos, especialmente diante da ausência, até então, de tipo penal específico voltado à invasão de dispositivos e à obtenção indevida de dados ou informações armazenadas em meio digital.[1]

A lei introduziu no Código Penal o art. 154-A, criando o tipo penal de invasão de dispositivo informático. A importância da norma não está apenas na proteção do aparelho eletrônico em si, mas na defesa dos dados, informações, imagens, comunicações e registros pessoais nele armazenados, que podem revelar aspectos da intimidade e da vida privada do usuário.

Antes da Lei n.º 12.737/2012, condutas como a invasão de computadores, a obtenção não autorizada de arquivos digitais ou o acesso indevido a dados pessoais eram, muitas vezes, analisadas a partir de figuras penais tradicionais, como furto, violação de correspondência, dano ou interrupção de serviço. Contudo, essa tentativa de enquadramento nem sempre era adequada, pois os dados digitais possuem natureza própria: podem ser copiados, reproduzidos e compartilhados sem que a vítima necessariamente perca a posse material do arquivo.[11]

A redação originária do art. 154-A exigia que a invasão ocorresse “mediante violação indevida de mecanismo de segurança”. Essa exigência foi criticada por restringir a incidência do tipo penal aos casos em que fosse demonstrada a superação de uma barreira técnica. Posteriormente, a Lei n.º 14.155/2021 alterou o art. 154-A do Código Penal, retirando do caput a exigência expressa de violação indevida de mecanismo de segurança e deslocando o foco da análise para a invasão não autorizada de dispositivo informático de uso alheio, com finalidade específica de obter, adulterar ou destruir dados ou informações, ou instalar vulnerabilidades para obtenção de vantagem ilícita.[21]

A Lei n.º 14.155/2021 também agravou as penas aplicáveis ao crime de invasão de dispositivo informático. Essa atualização demonstra que a Lei Carolina Dieckmann deve ser compreendida dentro de um processo de amadurecimento do Direito Penal Digital, marcado pela necessidade de adaptação às novas formas de criminalidade praticadas por meios tecnológicos.[22]

---

[11] PINHEIRO, Patrícia Peck. **Direito Digital**. 7. ed. São Paulo: Saraiva, 2021.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

A suficiência da Lei Carolina Dieckmann, portanto, deve ser interpretada de maneira relativa. A norma foi essencial para preencher lacuna legislativa e conferir tratamento penal próprio à invasão de dispositivo informático, mas não é suficiente, isoladamente, para proteger a privacidade na era digital. Sua eficácia depende da articulação com a Constituição Federal, o Código Civil, o Marco Civil da Internet, a LGPD, as normas penais posteriores e políticas de segurança digital.

Assim, a Lei Carolina Dieckmann mostra-se adequada como ponto de partida da tutela penal da privacidade digital, mas sua força normativa revela-se de forma mais consistente quando compreendida como parte de um ecossistema jurídico de proteção da pessoa na era digital.

2.6 Ciberstalking, exposição indevida de informações pessoais e novas violações à intimidade digital

Entre os riscos contemporâneos à privacidade no ambiente virtual, destacam-se o ciberstalking e a exposição indevida de informações pessoais. Essas práticas demonstram que a violação da intimidade digital não ocorre apenas pela invasão de dispositivos informáticos, mas também pela perseguição reiterada, pelo monitoramento abusivo e pela divulgação não autorizada de dados, imagens, conversas ou informações privadas.

A Lei Carolina Dieckmann, sancionada no final de 2012, representou a primeira resposta significativa do Código Penal Brasileiro direcionada especificamente aos crimes cibernéticos. Ela surgiu como resultado do impacto do caso da atriz homônima, cujo computador foi invadido, arquivos pessoais foram roubados e fotos íntimas foram divulgadas após tentativas de extorsão. A principal conquista dessa lei foi a inclusão do Artigo 154-A no Código Penal, que definiu o delito de Invasão de Dispositivo Informático, enfatizando que invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo,

Antes dessa lei, acessar o celular ou computador de outra pessoa sem permissão para obter dados pessoais não era considerado um crime. As vítimas precisavam recorrer a tipificações genéricas ou à esfera cível.

Importante enfatizar que a expressão ciberstalking, também chamado de ciberperseguição, consiste na perseguição reiterada praticada por meios digitais, como redes sociais, aplicativos de mensagens, e-mails, perfis falsos, softwares de monitoramento ou outras

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

ferramentas tecnológicas, com o objetivo de vigiar, constranger, ameaçar, intimidar ou perturbar a vítima. A expressão decorre da união entre *cyber*, relativo ao ambiente digital, e *stalking*, termo de origem inglesa utilizado para designar perseguição insistente ou obsessiva[12].

No ordenamento jurídico brasileiro, a perseguição foi tipificada pela Lei n.º 14.132/2021, que inseriu o art. 147-A no Código Penal[13]. O dispositivo pune a conduta de perseguir alguém, reiteradamente e por qualquer meio, ameaçando sua integridade física ou psicológica, restringindo sua capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Ao utilizar a expressão "por qualquer meio", o tipo penal alcança também condutas praticadas no ambiente digital, como envio insistente de mensagens, vigilância em redes sociais, criação de perfis falsos, ameaças virtuais e monitoramento indevido.

A Lei Carolina Dieckmann e a Lei do Stalking podem proteger aspectos da privacidade digital, mas atuam sobre condutas diferentes. A primeira volta-se à repressão da invasão não autorizada de dispositivo informático de uso alheio, com finalidade específica de obter, adulterar ou destruir dados ou informações, ou instalar vulnerabilidades para obtenção de vantagem ilícita. A segunda tem como núcleo a reiteração de condutas que invadem ou perturbam a liberdade e a privacidade da vítima, ainda que não haja invasão técnica de dispositivo.

Na prática, essas condutas podem coexistir, de modo que o agente pode invadir o e-mail, o celular ou uma conta digital da vítima para obter fotos, senhas, conversas ou dados pessoais e, posteriormente, utilizar essas informações para persegui-la, ameaçá-la ou constrangê-la reiteradamente. Nessa hipótese, a invasão de dispositivo informático e a perseguição digital podem configurar condutas autônomas, a depender do caso concreto.

Também merece atenção o uso de softwares de monitoramento abusivo, conhecidos como *stalkerware*. Trata-se de software espião instalado em celular, computador ou outro dispositivo para monitorar secretamente a atividade de uma pessoa, sem seu consentimento. Ele pode permitir acesso à localização, mensagens, chamadas, fotos, e-mails, senhas, histórico de

---

[12] MAIA, Daniel. **Criminalização do stalking no Brasil: análise do artigo 147-A do código penal em face do direito à privacidade**. Disponível em: <https://repositorio.ufc.br/handle/riufc/73074> Acesso em 11 jun. 2026.

[13] BRASIL. Lei Nº 14.132, De 31 de março de 2021. **Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais)**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm> Acesso em 12 jun. 2026.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

navegação e uso de aplicativos. Quando utilizado para acessar, vigiar ou extrair informações do dispositivo da vítima, pode aproximar-se do art. 154-A do Código Penal; se tais informações forem usadas para perseguir, ameaçar ou constranger a vítima, também poderá haver enquadramento no art. 147-A.

Essa relação demonstra que a proteção da privacidade digital não pode ser reduzida à proteção do aparelho, do sistema ou da senha. O dispositivo informático é, muitas vezes, apenas o meio pelo qual se acessam aspectos profundos da vida privada da pessoa. A violação digital pode atingir a intimidade, a autonomia, a liberdade, a reputação, a tranquilidade e a integridade psicológica da vítima.

A relação entre essas duas leis ocorre em três aspectos principais: progressão da conduta, meios de execução e o bem jurídico protegido.

O meio e o fim: invasão como instrumento de perseguição. A invasão de dispositivo, conduta tipificada pela Lei Carolina Dieckmann, é frequentemente utilizada como meio de execução ou escalada para o crime de cyberstalking.

Proteção da privacidade e intimidade. A proteção da privacidade, dignidade e liberdade individual no ecossistema digital é o núcleo comum de ambas as legislações. A Lei Carolina Dieckmann garante a segurança dos dados presentes nas ferramentas que utilizamos, ao passo que a Lei do Stalking resguarda a tranquilidade e a autodeterminação do indivíduo contra o assédio moral e o cerco virtual incessante.

Evolução histórica e doutrinária. A Lei 12.737/2012 permitiu que o legislador brasileiro reconhecesse que o ambiente virtual pode aumentar os danos psicológicos e morais. O cyberstalking é uma consequência direta dessa percepção: constatou-se que o criminoso virtual não se limita a "invadir o sistema" (como aborda a Lei Carolina Dieckmann), mas frequentemente utiliza a tecnologia de maneira contínua para encurralar, monitorar e incomodar a vítima (como estabelece a Lei 14.132/2021).

O progresso do Direito Digital no Brasil é caracterizado por respostas da legislação a casos de violência e violação da privacidade que se deslocaram para o meio virtual. A Lei Carolina Dieckmann e a subsequente criminalização do Cyberstalking são dois marcos importantes dessa trajetória. Apesar de abordarem comportamentos diferentes, elas possuem uma conexão histórica, lógica e progressiva significativa[14].

[14] FONTES, Jose Igor Alves. **Dados Pessoais Digitais e seu Tratamento No Ordenamento Jurídico Brasileiro**. Trabalho de Conclusão de Curso (Graduação em direito) -UFRN. Natal/RN: Biblioteca Setorial CCS, 2018. Disponível

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

O quadro 1, abaixo demonstra uma síntese comparativa das duas leis.

Quadro 1 – Análise comparativa Lei Carolina Dieckamn x 14.132/2021

Critério	Lei Carolina Dieckmann (Art. 154-A)	Lei do Stalking / Cyberstalking (Art. 147-A)
Foco da Conduta	O ato de invadir o dispositivo violando a segurança para obter/adulterar dados.	O ato de perseguir reiteradamente, gerando temor ou limitando a liberdade da vítima.
Temporalidade	Pode se consumar em um único ato de invasão.	Exige habitualidade (reiteração de mensagens, monitoramento ou tentativas de contato).
Ambiente	Estritamente ligado a dispositivos informáticos.	Pode ocorrer no ambiente físico, digital (*cyber*) ou em ambos cumulativamente.

Fonte: A autora, 2026

Em resumo, a Lei Carolina Dieckmann assegurou a proteção jurídica do "recinto privado digital" (como celular ou computador), ao passo que a criminalização do cyberstalking protege o indivíduo contra monitoramento e assédio obsessivo, tanto online quanto offline. As duas trabalham em conjunto para criar um ambiente digital mais seguro e menos hostil para as vítimas.

2.7 Desafios atuais para a proteção da privacidade digital

em: <https://monografias.ufrn.br/jspui/bitstream/123456789/7356/1/Dados%20Pessoais_Fontes_2018.pdf.> Acesso em: 05 jun. 2026.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

Na era digital, os desafios à privacidade tornaram-se mais complexos em razão da intensa circulação de informações pessoais em redes sociais, aplicativos, plataformas digitais, bancos de dados e sistemas automatizados. A coleta massiva de dados, a falta de transparência sobre as finalidades do tratamento, a dificuldade de obtenção de consentimento verdadeiramente informado e o aumento de vazamentos de dados estão entre os principais problemas enfrentados pelos titulares.[15]

A vulnerabilidade dos dados pessoais não decorre apenas de ataques técnicos sofisticados, como invasões de sistemas ou instalação de programas maliciosos. Ela também resulta de práticas cotidianas, como compartilhamento excessivo de informações, uso de senhas frágeis, aceitação automática de termos de uso, exposição de imagens íntimas ou familiares, preenchimento de cadastros em sites inseguros e interação com links fraudulentos. Tais situações criam ambiente propício para phishing, roubo de identidade, fraude eletrônica, invasão de dispositivo informático, exposição indevida de imagens e uso abusivo de dados pessoais.

A proteção da privacidade em redes sociais e plataformas digitais exige atuação em múltiplas frentes. Cabe ao Estado editar normas adequadas, fiscalizar sua aplicação e estruturar órgãos capazes de investigar e responsabilizar os autores de ilícitos digitais. Ao mesmo tempo, usuários, empresas e instituições devem adotar medidas de prevenção, segurança da informação e educação digital, pois a proteção da privacidade não se realiza apenas pela punição posterior ao dano, mas pela redução dos riscos que favorecem a violação de dados pessoais.

Além da dimensão preventiva, também existem desafios jurídicos relevantes, já que muitos delitos digitais ultrapassam fronteiras nacionais, dificultando a definição de jurisdição e a responsabilização dos autores. A coleta de evidências digitais também apresenta obstáculos específicos, pois os dados podem ser apagados, alterados, ocultados ou armazenados em servidores localizados em outros países. Soma-se a isso o uso de perfis falsos, mecanismos de anonimização e outras tecnologias de ocultação, que dificultam a identificação dos responsáveis.

Diante dessa realidade, o enfrentamento dos crimes cibernéticos exige cooperação institucional e internacional. A Convenção de Budapeste sobre o Crime Cibernético, promulgada no Brasil pelo Decreto n.º 11.491/2023, representa instrumento relevante de

---

[15] MEIRELES, Adriana Veloso. **Privacidade no século 21: proteção de dados, democracia e modelos regulatórios**. *Revista Brasileira de Ciência Política*. Disponível em: https://www.scielo.br/j/rbcpol/a/my3M8sH3tfpm4WmXhrNcMjK/. Acesso em: 27 out. 2025.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

colaboração entre Estados, especialmente diante da natureza transnacional de muitos delitos praticados no ambiente digital.[16]

Portanto, a proteção da privacidade digital não pode depender apenas da repressão penal posterior ao dano. É necessário combinar prevenção, educação digital, segurança da informação, proteção de dados pessoais, investigação especializada, cooperação institucional e mecanismos civis, administrativos e regulatórios. Somente uma resposta integrada é capaz de conferir maior efetividade à proteção da intimidade, da vida privada, da autodeterminação informativa e dos dados pessoais na sociedade digital.

A velocidade é o principal obstáculo no momento. Embora a lei exija um procedimento de investigação formal para comprovar a autoria e a materialidade do delito, a Inteligência Artificial possibilita que o autor elimine seus vestígios, altere seu IP ou crie uma nova identidade digital em questão de segundos.

Assim, a proteção atual se concentra na defesa proativa, em vez de "reagir" (esperar o crime ocorrer para processar). Isso inclui o uso de autenticação multifator (MFA), chaves de segurança físicas, ferramentas de criptografia ponta a ponta e, principalmente, a educação digital contínua para reconhecer fraudes psicológicas antes que o dispositivo seja comprometido.

3 considerações finais

O presente estudo teve como objetivo examinar o direito à privacidade na era digital a partir da análise da Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, avaliando sua importância, seus limites e sua inserção no conjunto normativo brasileiro de proteção da intimidade, da vida privada e dos dados pessoais.

Ao longo da pesquisa, verificou-se que a privacidade passou por significativa transformação conceitual. Inicialmente associada ao direito de ser deixado só, em uma perspectiva mais passiva de proteção contra intromissões indevidas, a privacidade passou a assumir, na sociedade digital, dimensão mais ativa, relacionada ao controle sobre o fluxo de informações pessoais. Nesse contexto, ganha relevância a noção de autodeterminação informativa, pela qual o indivíduo deve ter condições de compreender e influenciar a coleta, o uso, o compartilhamento, a conservação e a circulação de seus dados.

---

[16] BRASIL. **Decreto n.º 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada em Budapeste, em 23 de novembro de 2001.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

A Lei Carolina Dieckmann representou marco relevante para o Direito Penal brasileiro, pois introduziu no Código Penal o crime de invasão de dispositivo informático, conferindo resposta normativa específica a uma realidade até então tratada de forma insuficiente pelo ordenamento jurídico. Antes de sua edição, condutas envolvendo acesso indevido a computadores, celulares, contas digitais e arquivos pessoais eram frequentemente enquadradas em tipos penais tradicionais, nem sempre adequados à natureza dos bens atingidos no ambiente virtual.

Contudo, a suficiência da Lei n.º 12.737/2012 deve ser compreendida de forma relativa. A norma foi essencial como ponto de partida da tutela penal da privacidade digital, mas não é capaz, isoladamente, de enfrentar todos os riscos próprios da sociedade informacional. A redação originária do art. 154-A do Código Penal exigia a violação indevida de mecanismo de segurança, o que gerou críticas quanto à limitação de sua incidência. Com a alteração promovida pela Lei n.º 14.155/2021, essa exigência deixou de constar expressamente do caput do dispositivo, deslocando-se o foco para a invasão não autorizada de dispositivo informático de uso alheio, associada à finalidade específica de obter, adulterar ou destruir dados ou informações, ou instalar vulnerabilidades para obtenção de vantagem ilícita.

Essa alteração legislativa reforçou a tutela penal da privacidade digital, inclusive com o agravamento das penas aplicáveis. Ainda assim, a proteção da intimidade no ambiente virtual não pode depender exclusivamente da repressão penal posterior ao dano. A velocidade de disseminação de informações, a dificuldade de identificação dos autores, a volatilidade das provas digitais e a multiplicidade de formas de violação demonstram a necessidade de uma resposta jurídica mais ampla, preventiva e integrada.

Nesse cenário, a análise da Lei Carolina Dieckmann deve ser articulada com outros diplomas normativos. A Constituição Federal assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem, além de ter incorporado, por meio da Emenda Constitucional n.º 115/2022, a proteção de dados pessoais como direito fundamental autônomo. O Código Civil oferece instrumentos de prevenção, cessação e reparação de violações aos direitos da personalidade. O Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. A LGPD, por sua vez, disciplina tecnicamente o tratamento de dados pessoais, impondo deveres de segurança, transparência, prevenção e responsabilização aos agentes de tratamento.

Também se verificou que novas formas de violação da privacidade, como o ciberstalking e a exposição indevida de informações pessoais, ampliam a complexidade do tema. A Lei n.º 14.132/2021, ao tipificar o crime de perseguição, demonstra que a proteção da

pessoa no ambiente digital não se limita à defesa do dispositivo informático ou dos dados armazenados. A tutela jurídica deve alcançar também a liberdade, a tranquilidade, a integridade psicológica, a reputação e a segurança da vítima, especialmente diante de condutas reiteradas de vigilância, ameaça, constrangimento ou perturbação praticadas por meios digitais.

Conclui-se, portanto, que a Lei Carolina Dieckmann continua sendo instrumento relevante para a proteção penal da privacidade digital, mas sua efetividade depende de interpretação atualizada e de integração com o sistema constitucional, civil, administrativo e regulatório de proteção da pessoa. A privacidade na era digital não é protegida por uma única norma, mas por um ecossistema jurídico composto por regras penais, civis, constitucionais e de proteção de dados pessoais.

Dessa forma, a proteção da privacidade digital exige não apenas punição aos responsáveis por invasões de dispositivos informáticos, mas também educação digital, segurança da informação, prevenção de riscos, preservação adequada de provas, responsabilização civil e administrativa, além de fortalecimento da cultura de proteção de dados pessoais. O desafio contemporâneo consiste em equilibrar inovação tecnológica, liberdade de uso da internet e proteção da dignidade humana no ciberespaço.

Por fim, recomenda-se que estudos futuros aprofundem os impactos da inteligência artificial, da coleta massiva de dados, das decisões automatizadas e das novas formas de vigilância digital sobre a privacidade e a autodeterminação informativa. A constante evolução tecnológica impõe ao Direito o dever de atualização permanente, para que a tutela da intimidade, da vida privada e dos dados pessoais permaneça efetiva diante das novas formas de violação no ambiente digital.

Referências

ALMEIDA, Karen Rosa de. **Cyberstalking: do enquadramento atual à Necessidade de tutela específica – uma análise à luz do ordenamento jurídico brasileiro e do direito comparado**. Disponível em: <https://periodicos.ufba.br/index.php/rppgd/article/download/36359/24988/175050> Acesso em 25 out. 2025.

ASSUNÇÃO, Ana Paula Souza. **Crimes virtuais**. Disponível em: <http://repositorio.aee.edu.br/bitstream/aee/538/1/Monografia%20-%20Ana%20Paula%20Souza.pdf> Acesso em 22 out. 2025.

BARATTA, Alessandro. **Criminologia crítica e crítica do direito penal introdução à sociologia do direito penal**. 3. ed. Rio de Janeiro: Revan, 2002.

BIONI, Bruno. **Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de**

Defesa do Consumidor. civilistica.com, v. 9, n. 3, p. 1-23, 22 dez. 2020.

BISPO, Adrielle da Silva. **Crimes cibernéticos: da ineficácia da lei Carolina Dieckmann na prática de crimes virtuais**. Disponível em: <https://periodicorease.pro.br/rease/article/download/12291/5727/23272 Acesos em 28 out. 2025.

BRASIL, 2018. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em 2 out. 2025.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm> Acesso em: 20 out. 2025.

BRASIL. **Decreto-lei nº 3.914, de 9 de dezembro de 1941**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm> Acesso em 17 out. 2025.

BRASIL. Lei Nº 14.132, De 31 de março de 2021. **Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais)**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm> Acesso em 12 jun. 2026.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências, Brasília, DF. 3 dez.2012. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12737.htm> Acesso em: 24 out. 2025.

COLHADO, Junyor Gomes. **Conceito de crime no Direito Penal brasileiro**. Disponível em: <https://jus.com.br/artigos/47517/conceito-de-crime-no-direito-penalbrasileiro> Acesso em: 07 de mar. 2025.

COPETTI, Rafael; MIRANDA, Marcel Andreata De.et al. **Autodeterminação Informativa e Proteção de Dados: Uma Análise Crítica da Jurisprudência Brasileira. Direito, governança e novas tecnologias**. Florianópolis: CONPEDI, 2015. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/j6023guz-ncw4in57.pdf> Acesso em: 10 jun. 2026.

DENNY, Danielle Mendes Thame et al., **Direito Internacional na Era do Populismo Digital**. Disponível em: < https://revista.internetlab.org.br/direito-internacional-na-erado-populismo-digital/> Acesso em 29 out. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters, 2019.

FERNANDES, Aloir de Araújo. **Crimes na internet, lei Carolina Dieckmann e suas falhas**. Disponível em: < https://ri.unipac.br/repositorio/wp-content/uploads/tainacanitems/282/137736/ALOIR-DE-ARAUJO-FERNANDES-CRIMES-NA-INTERNET-LEI-CAROLINA-DIECKMANN-DIREITO-2015.pdf> Acesso em 30 out. 2025.

FONTES, Jose Igor Alves. **Dados Pessoais Digitais e seu Tratamento No Ordenamento Jurídico Brasileiro**. Trabalho de Conclusão de Curso (Graduação em direito) -UFRN. Natal/RN: Biblioteca Setorial CCS, 2018. Disponível em: <https://monografias.ufrn.br/jspui/bitstream/123456789/7356/1/Dados%20Pessoais_Fontes_2018.pdf.> Acesso em: 05 jun. 2026.

HINTZBERGEN, Jule. et al. **Fundamentos em Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Tradução Alan de Sá. Rio de Janeiro: Brasport, 2018.

MACHADO, Rafael Lopes Kassem. CRIMES CIBERNÉTICOS, INVASÃO DE PRIVACIDADE E A EFETIVIDADE DA RESPOSTA ESTATAL: os impactos da lei 12.737/2012 – lei Carolina Dieckmann e da lei geral de proteção de dados no combate aos crimes cibernéticos de invasão de privacidade. Disponível em: <https://projecaociencia.com.br/index.php/Projecao2/article/download/1798/1444> Acesso 20 out. 2025.

MAIA, Daniel. **Criminalização do stalking no Brasil: análise do artigo 147-A do código penal em face do direito à privacidade**. Disponível em: <https://repositorio.ufc.br/handle/riufc/73074> Acesso em 11 jun. 2026.

MASSON, Cleber. **Direito Penal esquematizado**. Editora Método, São Paulo, 2009.

MEIRELES, Adriana **Veloso. Privacidade no século 21: proteção de dados, democracia e modelos regulatórios**. Disponível em: <https://www.scielo.br/j/rbcpol/a/my3M8sH3tfpm4WmXhrNcMjK/> Acesso em 27 out. 2025.

MIRABETE, Julio Fabbrini; FABBRINI, Renato. **Manual de direito penal – parte geral**, v. I. 23ª ed. São Paulo: Atlas, 2006.

MUÉS, Gustavo Brandão Koury. **CRIMES VIRTUAIS: Uma análise sobre a adequação da legislação penal brasileira**. Disponível em:<https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf>
Acesso em: 19 out. 2025.

NETTO, Thaís. **Segurança da Informação: Mecanismos de Proteção Dentro das Organizações**. Disponível em: <https://direitoreal.com.br/artigos/seguranca-dainformacao-mecanismos-de-protecao-dentro-das-organizacoes> Acesso em: 22 out. 2025.

OTOBONI, Gustavo Henrique dos Santos**. Crimes cibernéticos: phishing. 2019**. Disponível em: <https://ambitojuridico.com.br/edicoes/revista191/crimesciberneticos-phishing/>. Acesso em 26 out. 2025.

PEIXOTO, Andréa Stefani. **Lei de Proteção de Dados: entenda em 13 pontos**!. Disponível em: <https://www.politize.com.br/lei-de-protecao-de-dados/> 2020, p .43. Acesso em 29 out. 2025.

PINHEIRO, Patrícia Peck. **Direito Digital**. 7ª ed. São Paulo: Saraiva, 2021.

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002.
SCHIMIDT, Guilherme. **Crimes Cibernéticos**. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em 26 out. 2025.

SILVA, Márcio Ferreira da. **Efetividade da Lei Carolina Dieckman**. Disponível em: <http://repositorio.aee.edu.br/bitstream/aee/17530/1/2017%20-TCC%20-%20MARCIO%20FERREIRA%20DA%20SILVA.pdf> Acesso em 30 out. 2025.

SILVA, Patrícia Santos da. **Direito cibernético e crime: análise da jurisdição de acordo com o lugar no julgamento de casos criminais**. Brasília: Vestnik, 2019.

SOUZA, Marcela Tavares et al. Revisão integrativa: o que é e como fazer. **Revista Einstein**. v. 8, p.102-106, 2010. Disponível em: <http://www.scielo.br/pdf/eins/v8n1/pt_1679-4508-eins-8-1-0102.pdf.> Acesso em: 20 out. 2025.

STEFAM, André. **Direito penal: parte geral** (arts. 1º a 120). São Paulo: Saraiva Educação, 2018.

TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico**. 5ª ed. São Paulo: Saraiva, 2020.

VIEIRA, Waleska Duque Estrada. A privacidade no ambiente cibernético: Direito fundamental do usuário. **Revista da ESMESC**, v. 24, n. 30, p. 197-217, 2017. Disponível em: https://revista. esmesc.org.br/re/article/view/167. Acesso em: 10 maio, 2026. DOI: https://doi.org/10.14295/revistadaesmesc.v24i30.p197