RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 06/10/2026 | Aceptado: 06/13/2026 | Publicación: 06/16/2026

El derecho a la privacidad en la era digital: un análisis de la Ley Carolina Dieckmann

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

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

Resumen:
Este artículo analiza el derecho a la privacidad en la era digital con base en la Ley N° 12.737/2012, conocida como Ley Carolina Dieckmann, examinando su importancia, sus límites y su articulación con el sistema brasileño para la protección de la intimidad, la vida privada y los datos personales. La investigación parte del siguiente problema: ¿hasta qué punto es efectiva la Ley Carolina Dieckmann 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 argumenta que la mencionada ley representó un hito indispensable para la protección penal de la privacidad digital, al criminalizar la invasión de dispositivos informáticos, pero su suficiencia es relativa, ya que la protección de la persona en el ciberespacio requiere una interpretación integrada con la Constitución Federal, el Código Civil, el Marco Civil da Internet (Carta de Derechos de Internet de Brasil), la Ley General de Protección de Datos Personales y legislación posterior, como la Ley N° 14.132/2021, que criminalizó el acoso cibernético. El objetivo general es evaluar la efectividad de la Ley Carolina Dieckmann en la protección de la privacidad digital. Los objetivos específicos incluyen: comprender la evolución del concepto de privacidad hacia la noción de autodeterminación informativa; analizar el delito de acceso no autorizado a dispositivos informáticos, tal como se define en el artículo 154-A del Código Penal; diferenciar la protección penal de la privacidad de las protecciones civiles, constitucionales y administrativas; 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 un enfoque cualitativo, basado en el análisis de la legislación, la doctrina y el contexto normativo relacionados con los ciberdelitos y la protección de datos personales. Se concluye que la Ley Carolina Dieckmann sigue siendo relevante como punto de partida para la protección penal de la privacidad digital, especialmente después de las enmiendas introducidas por la Ley N° 14.155/2021, que reforzó la respuesta penal al acceso no autorizado a dispositivos informáticos. Sin embargo, su eficacia depende de una comprensión sistémica y articulada, capaz de combinar la represión criminal, la prevención, la educación digital, la seguridad de la información, la responsabilidad civil y la protección de datos personales.

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

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**.**

1. Introducción

Las relaciones sociales contemporáneas se han transformado profundamente gracias a los avances en las tecnologías de la información y la comunicación. Actividades que antes se limitaban al espacio físico ahora se desarrollan en entornos digitales, como redes sociales, aplicaciones de mensajería, plataformas de almacenamiento, sistemas bancarios, servicios públicos electrónicos y dispositivos informáticos conectados a internet. Esta nueva realidad ha ampliado las posibilidades de comunicación, acceso a la información y participación social, pero también ha intensificado los riesgos de vulneración de la privacidad, la vida privada, el honor, la imagen y los datos personales [1].

En este contexto, el derecho a la privacidad, garantizado por la Constitución Federal de 1988, ha comenzado a enfrentar desafíos propios de la sociedad digital. La vida privada ya no se concentra únicamente en espacios físicos o documentos materiales, sino que se proyecta en teléfonos celulares, computadoras, cuentas digitales, bases de datos, plataformas en línea y sistemas de comunicación en red. Como resultado, las intrusiones en dispositivos, el acceso no autorizado, la exposición de imágenes, la divulgación no autorizada de información personal, el phishing , el robo de credenciales, el fraude digital y el ciberacoso representan amenazas concretas a la dignidad humana.

Históricamente, el sistema jurídico brasileño ha enfrentado dificultades para tipificar como delito ciertas conductas cometidas en el entorno informático. Antes de la Ley N° 12.737/2012, conocida como Ley Carolina Dieckmann, la intrusión en dispositivos y la obtención ilícita de archivos digitales se analizaban frecuentemente con base en delitos penales tradicionales, que no siempre se ajustaban a la naturaleza de los datos e información almacenados electrónicamente. Esta dificultad generaba inseguridad jurídica, especialmente

[1]COPETTI, Rafael; MIRANDA, Marcel Andreata De. et al. **Autodeterminación informacional y protección de datos: un análisis crítico de la jurisprudencia brasileña. Derecho, gobernanza y nuevas tecnologías** . Florianópolis: CONPEDI, 2015. Disponible en: < http://www.egov.ufsc.br/portal/sites/default/files/j6023guzncw4in57.pdf > Consultado el 10 de junio de 2026.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 06/10/2026 | Aceptado: 06/13/2026 | Publicación: 06/16/2026

porque los datos digitales pueden copiarse, reproducirse o compartirse sin que ello implique necesariamente la sustracción física del bien.

La Ley N° 12.737/2012 surgió, por lo tanto, como una respuesta legislativa pertinente a una laguna específica en el Derecho Penal brasileño, al introducir el delito de acceso no autorizado a dispositivos informáticos en el Código Penal. Su promulgación fue motivada por un caso de gran repercusión que involucró la exposición indebida de la privacidad de una persona de renombre nacional, lo que puso de manifiesto la necesidad de una protección penal más adecuada contra el acceso no autorizado a dispositivos e información personal.

A pesar de su importancia histórica, la Ley Carolina Dieckmann no puede analizarse de forma aislada. La evolución tecnológica, la aparición de nuevas formas de delitos digitales y la expansión del marco normativo para la protección de la privacidad exigen una interpretación integral. La Constitución Federal protege la intimidad, la vida privada, el honor y la imagen; la Enmienda Constitucional N° 115/2022 incluyó la protección de datos personales como un derecho fundamental autónomo; el Marco Civil da Internet (Carta de Derechos de Internet de Brasil) establece principios, garantías, derechos y deberes para el uso de Internet; la Ley General de Protección de Datos regula el tratamiento de datos personales; y el Código Penal ha sufrido actualizaciones adicionales, como la Ley N° 14.155/2021, que modificó el Artículo 154-A, y la Ley N° 14.132/2021, que penalizó el acoso.

En este contexto, el problema central de esta investigación consiste en determinar hasta qué punto la Ley N° 12.737/2012 es eficaz para proteger la privacidad en la era digital, considerando los cambios legislativos posteriores, la autonomía constitucional de la protección de datos personales y la complejidad técnica de los ciberdelitos. La hipótesis planteada es que la Ley Carolina Dieckmann representó un hito indispensable para la protección penal de la privacidad digital, pero su suficiencia es relativa, ya que la protección efectiva del individuo en el entorno virtual depende de la articulación entre la represión penal, la protección civil, la protección constitucional, la seguridad de la información, la educación digital y el régimen jurídico para la protección de datos personales.

El objetivo general de este estudio es evaluar la efectividad de la Ley Carolina Dieckmann en la protección de la privacidad digital. Los objetivos específicos incluyen: comprender la evolución del concepto de privacidad hacia la noción de autodeterminación informativa; analizar el delito de acceso no autorizado a un dispositivo informático según lo define el Artículo 154-A del Código Penal; examinar los cambios introducidos por la Ley No. 14.155/2021; distinguir entre la protección penal de la privacidad y las protecciones civiles, constitucionales y administrativas; y relacionar la Ley Carolina Dieckmann con otros

instrumentos normativos relevantes, como la Carta de Derechos de Internet de Brasil (Marco Civil da Internet), la Ley General de Protección de Datos de Brasil (LGPD) y la Ley contra el Acoso .

La metodología adoptada es bibliográfica y documental, con un enfoque cualitativo. La investigación se basa en el análisis de la legislación brasileña, la doctrina especializada y las normas relativas a la protección de la privacidad, los datos personales y la lucha contra los ciberdelitos. El estudio parte de una perspectiva jurídico-dogmática, buscando comprender los límites y las posibilidades de la protección penal de la privacidad en el entorno digital, sin descuidar la necesaria articulación con otros mecanismos de protección del individuo.

La relevancia de esta investigación se justifica por la creciente exposición de las personas a los riesgos digitales y la necesidad de comprender cómo la ley puede responder a las nuevas formas de violación de la privacidad y los datos personales. El análisis de la Ley Carolina Dieckmann permite verificar los avances logrados por la legislatura brasileña, pero también pone de relieve que la protección de la privacidad en la era digital no depende únicamente del castigo tras la intrusión en los dispositivos. Requiere, asimismo, prevención, educación digital, seguridad de la información, responsabilidad civil y administrativa, cooperación institucional y el fortalecimiento de la cultura de protección de datos personales.

Más allá de la invasión de dispositivos informáticos, la investigación también aborda prácticas como el ciberacoso y la divulgación indebida de información personal, ya que dicha conducta demuestra que la privacidad digital puede ser vulnerada tanto por el acceso no autorizado a datos almacenados como por el acoso reiterado, la vigilancia abusiva, las amenazas de divulgación de información y la restricción de la libertad de la víctima en el entorno virtual. Esta ampliación del debate es fundamental para comprender que la protección jurídica contemporánea no debe limitarse a la protección de los equipos electrónicos, sino que debe extenderse a la persona, su privacidad, su autonomía, su libertad, su integridad psicológica y su autodeterminación informativa.

Por lo tanto, este trabajo busca demostrar que la Ley Carolina Dieckmann sigue siendo relevante para la protección penal de la privacidad digital, pero debe entenderse como parte de un ecosistema normativo más amplio. La efectividad de la protección de las personas en la era digital depende de la interacción entre la Constitución Federal, el Código Civil, el Marco Civil da Internet (Ley de Derechos de Internet de Brasil), la LGPD (Ley General de Protección de Datos de Brasil), el Código Penal y la legislación específica destinada a abordar nuevas formas de violación de la intimidad, la vida privada y los datos personales.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 06/10/2026 | Aceptado: 06/13/2026 | Publicación: 06/16/2026

2. Marco teórico

2.1 Privacidad, intimidad y protección de datos personales en la sociedad digital

La protección de la privacidad y la intimidad es un derecho fundamental garantizado por la Constitución Federal de 1988, especialmente en el artículo 5, inciso X, que reconoce la inviolabilidad de la intimidad, la vida privada, el honor y la imagen de las personas, asegurando la indemnización por los daños materiales o morales que resulten de su violación. En el entorno digital, esta protección adquiere especial relevancia, ya que la vida privada se proyecta en dispositivos informáticos, redes sociales, aplicaciones de mensajería, plataformas digitales, bases de datos y sistemas de comunicación en red.

Tradicionalmente, el derecho a la privacidad se ha entendido desde una perspectiva negativa, asociado al «derecho a que te dejen en paz», es decir, la protección del individuo contra intrusiones indebidas en su esfera privada. Sin embargo, esta concepción se ha vuelto insuficiente ante la sociedad de la información y el avance de las tecnologías de la información y la comunicación.[2]

En el ámbito digital, la privacidad también ha llegado a implicar una dimensión activa de control sobre la información personal, que abarca la posibilidad de que las personas influyan en el acceso, la exposición, el intercambio, la finalidad y el uso de los datos relacionados con sus vidas personales.

Esta evolución conduce al concepto de autodeterminación informativa, entendida como el derecho de una persona a ejercer control sobre sus propios datos e información personal, supervisando e influyendo en cómo se recopilan, utilizan, almacenan, comparten y eliminan. [3]De este modo, el titular de los datos deja de ser simplemente alguien protegido contra intrusiones indebidas y pasa a ser reconocido como un sujeto activo en el control de la circulación de su información.

---

[2]DONEDA, Danilo Cesar Maganhoto . **De la privacidad a la protección de datos personales: elementos de la formación del Reglamento General de Protección de Datos** . 2.ª ed. São Paulo: Thomson Reuters Brasil, 2020. Véase también: COOLEY, Thomas McIntyre . **Tratado sobre el derecho de daños, o los agravios que surgen independientemente del contrato** . Chicago: Callaghan and Company, 1879; WARREN, Samuel D.; BRANDEIS, Louis D. **El derecho a la privacidad** . *Harvard Law Review* , vol. 4, n.º 5, págs. 193-220, 1890.

[3]MENKE, Fabiano. **Orígenes alemanes y el significado de la autodeterminación informativa** . *Migalhas* , 30 de octubre de 2020; DONEDA, Danilo César Maganhoto . **De la privacidad a la protección de datos personales** . 2da ed. São Paulo: Thomson Reuters Brasil, 2020.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 06/10/2026 | Aceptado: 06/13/2026 | Publicación: 06/16/2026

En este contexto, es necesario distinguir entre privacidad y protección de datos personales. La privacidad protege la esfera íntima, la vida privada y la intimidad personal de un individuo frente a la exposición, interferencia o intrusión indebidas. La protección de datos personales, por su parte, abarca cualquier información relativa a una persona física identificada o identificable, incluso si dicha información no es, en sí misma, íntima o sensible. Datos como el nombre, el CPF (número de identificación fiscal brasileño), la ubicación, la dirección de correo electrónico, los registros de acceso, los hábitos de navegación y el perfil de consumo pueden no revelar directamente la intimidad de una persona, pero su manejo inadecuado puede afectar su libertad, autonomía, dignidad y autodeterminación informativa.

La Enmienda Constitucional N° 115/2022 consolidó esta evolución al incluir en el artículo 5, inciso LXXIX, de la Constitución Federal, el derecho fundamental a la protección de datos personales, incluso en medios digitales. [4]Con ello, la protección de datos quedó expresamente incluida en el catálogo de derechos fundamentales, sin confundirse con la privacidad, aunque históricamente vinculada a ella.

Así pues, en el entorno virtual, la protección de la privacidad, la intimidad y los datos personales es fundamental para preservar la libertad y la dignidad humana. La divulgación indebida de información, el pirateo de dispositivos, el mal uso de datos y la falta de transparencia en el manejo de la información personal pueden comprometer no solo la esfera privada de un individuo, sino también su autonomía, seguridad, reputación y capacidad para participar libremente en la vida social.[5]

2.2 Protección civil-constitucional de la privacidad digital

En Brasil, la protección de la privacidad tiene un fundamento civil-constitucional. Esto significa que la privacidad no debe entenderse simplemente como un interés individual disponible o como una simple relación entre particulares, sino como un derecho fundamental vinculado a la dignidad humana, la libertad, la intimidad y el libre desarrollo de la personalidad.

En el plano constitucional, el artículo 5, inciso X, de la Constitución Federal garantiza la inviolabilidad de la privacidad, la vida privada, el honor y la imagen. El inciso XII del mismo

[4]BRASIL. **Enmienda Constitucional N° 115, del 10 de febrero de 2022.** Modifica la Constitución Federal para incluir la protección de datos personales entre los derechos y garantías fundamentales.

[5]RODOTÀ, Stefano. **La vida en la sociedad de vigilancia: la privacidad hoy** . Río de Janeiro: Renovar, 2008; BIONI, Bruno Ricardo. **Regulación y protección de datos personales: el principio de responsabilidad** . Río de Janeiro: Forense, 2022.

artículo protege asimismo el secreto de la correspondencia y las comunicaciones telegráficas, digitales y telefónicas, salvo en procesos judiciales y por orden judicial, cuando corresponda. Estas disposiciones constituyen el fundamento constitucional para la protección de la vida privada, incluso en el ámbito digital.

En derecho civil, el Código Civil concreta esta protección mediante los derechos de la personalidad, estableciendo en su artículo 21 que la vida privada de la persona natural es inviolable, y autorizando al juez, a petición del interesado, a adoptar las medidas necesarias para prevenir o detener cualquier acto contrario a esta norma. El artículo 187 considera ilícito el ejercicio abusivo de un derecho, especialmente cuando el titular excede los límites impuestos por la buena fe, la moral o la finalidad económica y social del derecho.

Así, la intrusión en dispositivos informáticos, el acceso no autorizado a cuentas personales, la divulgación no autorizada de imágenes, el intercambio abusivo de información privada y el uso indebido de datos personales pueden constituir no solo delitos penales, sino también delitos civiles. En el ámbito penal, se requiere una tipificación estricta; en el ámbito civil, la protección es más amplia, ya que busca prevenir, detener o remediar las violaciones de los derechos de la personalidad.

Este entendimiento es relevante para la presente investigación porque demuestra que la Ley Carolina Dieckmann no actúa de forma aislada. Forma parte de un sistema más amplio para la protección de las personas en la era digital, compuesto por la Constitución Federal, el Código Civil, el Marco Civil da Internet (Ley de Derechos de Internet de Brasil), la LGPD (Ley General de Protección de Datos de Brasil) y leyes penales específicas destinadas a abordar la conducta en el entorno virtual.

2.3 Marco regulatorio para la protección de la privacidad en el entorno digital

La Carta de Derechos de Internet de Brasil (Marco Civil da Internet), Ley N° 12.965/2014, representa un hito normativo importante para el uso de internet en Brasil. Su relevancia radica en que establece principios, garantías, derechos y deberes aplicables al entorno digital, funcionando como un marco normativo orientado a la organización jurídica de las relaciones que se desarrollan en la red.

Esta legislación se basa principalmente en principios que buscan establecer parámetros generales para el uso de internet en el país. El artículo 3 de la Carta Brasileña de Derechos de Internet establece, entre sus principios, la garantía de la libertad de expresión, comunicación y manifestación del pensamiento, la protección de la privacidad, la protección de datos personales

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 06/10/2026 | Aceptado: 06/13/2026 | Publicación: 06/16/2026

"según lo dispuesto por la ley", la preservación y garantía de la neutralidad de la red, la estabilidad, seguridad y funcionalidad de la red, así como la responsabilidad de los agentes según sus actividades.

Por este motivo, el Marco Civil de Internet (BCD) no debe considerarse un régimen general para la protección de datos personales. Anticipa y estructura principios esenciales para la protección de los derechos de los usuarios en internet, creando una base normativa que posteriormente fue ampliada por la LGPD (Ley General de Protección de Datos de Brasil). En este sentido, puede entenderse como una especie de "Constitución de Internet", que establece fundamentos y directrices generales para el entorno digital, sin sustituir la disciplina técnica específica de la protección de datos personales.[6]

La Ley General de Protección de Datos, Ley N° 13.709/2018, a su vez, representa el principal marco jurídico brasileño que regula el tratamiento de datos personales. Su finalidad es proteger los derechos fundamentales de libertad, privacidad y libre desarrollo de la personalidad de la persona física, estableciendo normas aplicables a las operaciones de tratamiento realizadas por personas físicas o jurídicas, de derecho público o privado, en soportes físicos o digitales. ¹¹

La LGPD (Ley General de Protección de Datos de Brasil) no tiene carácter penal y no debe entenderse como una ley genérica de privacidad. Se trata de una norma técnica, basada en principios y de procedimiento, cuyo objetivo es regular las actividades de recopilación, almacenamiento, uso, intercambio, eliminación y otras formas de tratamiento de datos personales. Mientras que la Ley Carolina Dieckmann opera en el ámbito penal, al criminalizar la intrusión en dispositivos informáticos, la LGPD actúa en una dimensión preventiva, regulatoria, administrativa y civil, regulando cómo deben tratarse los datos personales de manera lícita, transparente, segura y responsable.[7]

Entre los principios de la LGPD (Ley General de Protección de Datos de Brasil), destacan los siguientes: finalidad, adecuación, necesidad, libre acceso, calidad de los datos, transparencia, seguridad, prevención, no discriminación y responsabilidad. La ley también

---

[6]ASSIS, Ana Cláudia Miranda Lopes. **Cumplimiento digital y protección de datos en la educación primaria: un análisis desde la perspectiva de la LGPD sobre los desafíos y perspectivas para la educación pública en el municipio de Porto Velho–RO** . 2024. Tesis (Doctorado en Derecho) – Pontificia Universidad Católica de Rio Grande do Sul, Porto Alegre, 2024. Disponible en: https://tede2.pucrs.br/tede2/handle/tede/12012 . Consultado el 14 de mayo de 2026.

[7]BRASIL. **Ley N° 13.709, de 14 de agosto de 2018** , arts . 1, 5, 6, 7, 18, 42 y 46; PECK, Patricia Pinheiro. **Protección de Datos Personales: comentarios a la Ley N° 13.709/2018 (LGPD)** . 4ª edición. São Paulo: SaraivaJur , 2023.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 06/10/2026 | Aceptado: 06/13/2026 | Publicación: 06/16/2026

garantiza los derechos del titular de los datos, tales como la confirmación de la existencia del tratamiento, el acceso, la rectificación, la anonimización, el bloqueo, la supresión, la portabilidad, la información sobre el intercambio de datos, la revocación del consentimiento y la oposición al tratamiento irregular.[1]

Por lo tanto, el Marco Civil de Internet (CCI) y la Ley General de Protección de Datos (LGPD) cumplen funciones distintas y complementarias. El primero establece principios generales para el uso de internet; el segundo regula técnicamente el tratamiento de datos personales. Sin embargo, ambos forman parte del mismo marco normativo para la protección de las personas en el entorno digital.

2.4 Delitos cibernéticos y protección penal de la privacidad

La evolución tecnológica ha modificado profundamente las formas de interacción social, económica y comunicacional, pero también ha incrementado los riesgos de vulnerar los derechos fundamentales. Internet y los dispositivos informáticos se utilizan no solo como instrumentos de comunicación y acceso a la información, sino también como medios para llevar a cabo conductas ilícitas que atentan contra la privacidad, la propiedad, el honor, la libertad y la seguridad de las personas.

Los ciberdelitos pueden entenderse como conductas delictivas cometidas mediante el uso de ordenadores, redes informáticas, dispositivos electrónicos, sistemas de información o entornos digitales. Estos medios pueden funcionar como instrumentos para cometer el delito o constituir el objeto mismo de la conducta delictiva.[8]

La doctrina jurídica suele distinguir entre ciberdelitos lícitos e ilícitos. Los ciberdelitos lícitos son aquellos en los que el entorno digital , los sistemas informáticos o los datos electrónicos son parte integral del delito, como en el caso del acceso no autorizado a un dispositivo informático. Los ciberdelitos ilícitos, por otro lado, corresponden a delitos tradicionales cometidos a través de internet o tecnologías digitales, como el fraude, las

[8]COLLI, Maciel. **Ciberdelitos: límites y perspectivas de la investigación policial de los ciberdelitos** . Curitiba: Juruá, 2010; ROSSINI, Augusto Eduardo de Souza. **Informática, telemática y derecho penal** . São Paulo: Memoria Jurídica, 2004.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 06/10/2026 | Aceptado: 06/13/2026 | Publicación: 06/16/2026

amenazas, la difamación, la divulgación no autorizada de imágenes y otras conductas que podrían ocurrir fuera del entorno virtual, pero que se ven amplificadas por la tecnología.[9]

Los delitos digitales presentan desafíos específicos, como la rapidez con la que se ejecutan, la veloz difusión de la información, la dificultad para identificar a los autores, la volatilidad de las pruebas digitales, el carácter transnacional de ciertas prácticas y la necesidad de conocimientos especializados. Estos elementos demuestran que la lucha contra los ciberdelitos requiere no solo la represión criminal, sino también la prevención, la educación digital, la seguridad de la información, la cooperación institucional y la actualización constante de la legislación.[10]

2.5 La Ley Dieckmann de Carolina y la invasión de dispositivos informáticos

La Ley N° 12.737/2012, conocida como Ley Carolina Dieckmann, representa un hito significativo en la evolución de la protección penal de la privacidad digital en Brasil. Su promulgación se produjo en un contexto de creciente exposición de las personas a los riesgos derivados del uso de computadoras, teléfonos celulares, redes sociales, aplicaciones y otros dispositivos de información, especialmente dada la ausencia, hasta entonces, de un delito específico dirigido a la intrusión en dispositivos y la obtención indebida de datos o información almacenada digitalmente.[1]

La ley introdujo el artículo 154-A en el Código Penal, tipificando como delito el acceso no autorizado a un dispositivo informático. La importancia de esta norma radica no solo en la protección del dispositivo electrónico en sí, sino también en la salvaguarda de los datos, la información, las imágenes, las comunicaciones y los registros personales almacenados en él, que pueden revelar aspectos de la privacidad y la vida privada del usuario.

Antes de la Ley N° 12.737/2012, acciones como el pirateo informático, la obtención no autorizada de archivos digitales o el acceso indebido a datos personales solían analizarse según delitos penales tradicionales como el hurto, la violación de correspondencia, los daños o la interrupción del servicio. Sin embargo, este intento de clasificación no siempre era adecuado,

---

[9]WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Ciberdelitos: amenazas y procedimientos de investigación** . 2da ed. Río de Janeiro: Brasport , 2013; ROSA, Fabrizio Rosa. **Ciberdelitos: aspectos penales y procesales** . São Paulo: JH Mizuno, 2017.

[10]MARCELI, Vilma Maria; DAHER, Roberto José. **Análisis evolutivo de los ciberdelitos y el derecho penal brasileño** . *FACP Electronic Journal* , año XV, n.º 28, págs. 100-116, marzo de 2026.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 06/10/2026 | Aceptado: 06/13/2026 | Publicación: 06/16/2026

ya que los datos digitales tienen una naturaleza propia: pueden copiarse, reproducirse y compartirse sin que la víctima pierda necesariamente la posesión física del archivo.[11]

La redacción original del artículo 154-A exigía que la intrusión se produjera "mediante la violación indebida de un mecanismo de seguridad". Este requisito fue criticado por restringir la aplicación del delito a los casos en que se demostraba la superación de una barrera técnica. Posteriormente, la Ley n.º 14.155/2021 modificó el artículo 154-A del Código Penal, eliminando el requisito expreso de la violación indebida de un mecanismo de seguridad del texto principal y centrando el análisis en la intrusión no autorizada en el dispositivo informático de otra persona, con el propósito específico de obtener, alterar o destruir datos o información, o instalar vulnerabilidades para obtener una ventaja ilícita.[2 1]

La Ley N° 14.155/2021 también incrementó las penas aplicables al delito de acceso no autorizado a un sistema informático. Esta actualización demuestra que la Ley Carolina Dieckmann debe entenderse dentro de un proceso de maduración del Derecho Penal Digital, marcado por la necesidad de adaptarse a las nuevas formas de delincuencia cometidas a través de medios tecnológicos.[2 2]

Por lo tanto, la suficiencia de la Ley Carolina Dieckmann debe interpretarse de forma relativa. Si bien la ley fue esencial para subsanar una laguna legislativa y proporcionar un tratamiento penal específico para la invasión de dispositivos informáticos, no basta, por sí sola, para proteger la privacidad en la era digital. Su efectividad depende de su articulación con la Constitución Federal, el Código Civil, el Marco Civil da Internet (Ley de Derechos de Internet de Brasil), la LGPD (Ley General de Protección de Datos de Brasil), las leyes penales posteriores y las políticas de seguridad digital.

Así pues, la Ley Carolina Dieckmann demuestra ser adecuada como punto de partida para la protección penal de la privacidad digital, pero su fuerza normativa se revela de forma más consistente cuando se entiende como parte de un ecosistema jurídico para la protección del individuo en la era digital.

2.6 Ciberacoso , divulgación indebida de información personal y nuevas violaciones de la privacidad digital.

destacan el ciberacoso y la divulgación indebida de información personal . Estas prácticas demuestran que la violación de la privacidad digital no solo se produce mediante la

[11]PINHEIRO, Patricia Peck. **Derecho Digital** . 7ª edición. São Paulo: Saraiva, 2021.

intrusión en dispositivos informáticos, sino también a través del acoso reiterado, la vigilancia abusiva y la divulgación no autorizada de datos, imágenes, conversaciones o información privada.

La Ley Carolina Dieckmann, promulgada a finales de 2012, representó la primera respuesta significativa del Código Penal brasileño dirigida específicamente a los ciberdelitos. Surgió a raíz del caso de la actriz homónima, cuyo ordenador fue pirateado, sus archivos personales robados y sus fotos íntimas difundidas tras intentos de extorsión. El principal logro de esta ley fue la inclusión del artículo 154-A en el Código Penal, que define el delito de invasión informática, estableciendo que invadir el dispositivo informático de otra persona, esté o no conectado a una red informática, mediante la violación indebida de los mecanismos de seguridad y con el propósito de obtener, alterar o destruir datos o información sin la autorización expresa o tácita del propietario del dispositivo, constituye un delito.

Antes de esta ley, acceder al teléfono móvil o al ordenador de otra persona sin permiso para obtener datos personales no se consideraba delito. Las víctimas tenían que recurrir a clasificaciones genéricas o al ámbito civil.

Es importante destacar que el término ciberacoso , también llamado ciberhostigamiento , consiste en el acoso reiterado realizado a través de medios digitales, como redes sociales, aplicaciones de mensajería, correos electrónicos, perfiles falsos, software de monitoreo u otras herramientas tecnológicas, con el objetivo de vigilar, acosar, amenazar, intimidar o perturbar a la víctima. La expresión proviene de la combinación de *ciber* , que se refiere al entorno digital, y *hostigamiento* , un término de origen inglés que designa el acoso persistente u obsesivo [12].

En el ordenamiento jurídico brasileño, el acoso fue tipificado como delito por la Ley N° 14.132/2021, que incorporó el artículo 147-A al Código Penal [13]. Este artículo castiga el acoso reiterado a una persona por cualquier medio, amenazando su integridad física o psicológica, restringiendo su libertad de movimiento o invadiendo o perturbando de cualquier otra forma su libertad o privacidad. Al utilizar la expresión "por cualquier medio", el delito también abarca

[12] MAIA, Daniel. **Criminalización del** acoso **en Brasil: análisis del artículo 147-** A **del código penal a la luz del derecho a la privacidad** . Disponible en: <https://repositorio.ufc.br/handle/riufc/73074 >. Consultado el 11 de junio de 2026.
[13]BRASIL. Ley N° 14.132, del 31 de marzo de 2021. **Añade el artículo 147-A al Decreto Ley N° 2.848, del 7 de diciembre de 1940 (Código Penal), para tipificar el delito de acoso; y deroga el artículo 65 del Decreto Ley N° 3.688, del 3 de octubre de 1941 (Ley de Delitos Penales)** . Disponible en: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm> Consultado el 12 de junio de 2026.

conductas realizadas en el entorno digital, como el envío persistente de mensajes, la vigilancia en redes sociales, la creación de perfiles falsos, las amenazas virtuales y el monitoreo indebido.

la Ley Dieckmann de Carolina como la Ley contra el Acoso protegen aspectos de la privacidad digital, pero abordan distintos tipos de conducta. La primera se centra en impedir la invasión no autorizada del dispositivo informático de otra persona, con el propósito específico de obtener, alterar o destruir datos o información, o de instalar vulnerabilidades para obtener una ventaja ilícita. La segunda se centra en la conducta reiterada que invade o perturba la libertad y la privacidad de la víctima, incluso si no hay una intrusión técnica en el dispositivo.

En la práctica, estas conductas pueden coexistir, de modo que el agresor puede acceder al correo electrónico, teléfono móvil o cuenta digital de la víctima para obtener fotos, contraseñas, conversaciones o datos personales, y posteriormente utilizar esta información para acosarla, amenazarla o hostigarla repetidamente. En este caso, el acceso no autorizado a un dispositivo informático y el acoso digital pueden constituir acciones distintas, según las circunstancias.

También merece atención el uso de software de vigilancia abusivo, conocido como *stalkerware* . Se trata de software espía instalado en un teléfono celular, computadora u otro dispositivo para monitorear secretamente la actividad de una persona sin su consentimiento. Puede permitir el acceso a la ubicación, mensajes, llamadas, fotos, correos electrónicos, contraseñas, historial de navegación y uso de aplicaciones. Cuando se utiliza para acceder, monitorear o extraer información del dispositivo de la víctima, puede estar tipificado en el Artículo 154-A del Código Penal; si dicha información se utiliza para acosar, amenazar o hostigar a la víctima, también puede estar tipificado en el Artículo 147-A.

Esta relación demuestra que la protección de la privacidad digital no se reduce a la protección del dispositivo, el sistema o la contraseña. El dispositivo informático suele ser simplemente el medio por el cual se accede a aspectos profundos de la vida privada de una persona. La violación digital puede afectar la intimidad, la autonomía, la libertad, la reputación, la tranquilidad y la integridad psicológica de la víctima.

La relación entre estas dos leyes se manifiesta en tres aspectos principales: la progresión de la conducta, los medios de ejecución y el interés jurídico protegido.

El medio y el fin: el hackeo como herramienta de persecución. El hackeo de dispositivos, una conducta tipificada por la Ley Dieckmann de Carolina, se utiliza con frecuencia como medio de ejecución o escalada del delito de ciberacoso .

Protección de la privacidad y la intimidad. La protección de la privacidad, la dignidad y la libertad individual en el ecosistema digital constituye el núcleo común de ambas leyes. La

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 06/10/2026 | Aceptado: 06/13/2026 | Publicación: 06/16/2026

Ley Carolina Dieckmann garantiza la seguridad de los datos presentes en las herramientas que utilizamos, mientras que la Ley contra el Acoso protege la tranquilidad y la autodeterminación del individuo frente al acoso moral y la vigilancia virtual constante.

Evolución histórica y doctrinal. La Ley 12.737/2012 permitió al legislador brasileño reconocer que el entorno virtual puede incrementar el daño psicológico y moral. El ciberacoso es una consecuencia directa de esta percepción: se ha constatado que el ciberdelincuente no se limita a "invadir el sistema" (como lo aborda la Ley Carolina Dieckmann), sino que frecuentemente utiliza la tecnología de forma continua para acorralar, vigilar y acosar a la víctima (como establece la Ley 14.132/2021).

El progreso del Derecho Digital en Brasil se caracteriza por respuestas legislativas a casos de violencia y violaciones de la privacidad que se han trasladado al entorno virtual. La Ley Carolina Dieckmann y la posterior penalización del ciberacoso constituyen dos hitos importantes en esta trayectoria. Si bien abordan conductas diferentes, comparten una conexión histórica, lógica y progresiva significativa [14].

La tabla 1 que aparece a continuación muestra un resumen comparativo de las dos leyes.

Tabla 1 – Análisis comparativo de la Ley Carolina Dieckmann vs. Ley 14.132/2021

Criterio	Ley Carolina Dieckmann (Art. 154-A)	Ley contra el acoso / ciberacoso (Artículo 147-A)
Enfoque de la conducta	El acto de piratear un dispositivo vulnerando su seguridad para obtener o alterar datos.	El acto de acosar repetidamente, generando miedo o limitando la libertad de la víctima.
Temporalidad	Puede lograrse con un solo acto de invasión.	Requiere regularidad (mensajes repetidos, seguimiento o intentos de contacto).

[14]FONTES, Jose Igor Alves. **Datos personales digitales y su tratamiento en el ordenamiento jurídico brasileño** . Tesis de grado (Derecho) - UFRN. Natal/RN: Biblioteca Sectorial CCS, 2018. Disponible en: < https://monografias.ufrn.br/jspui/bitstream/123456789/7356/1/Dados%20Pessoais_Fontes_2018.pdf >. Consultado el 5 de junio de 2026.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 06/10/2026 | Aceptado: 06/13/2026 | Publicación: 06/16/2026

Criterio	Ley Carolina Dieckmann (Art. 154-A)	Ley contra el acoso / ciberacoso (Artículo 147-A)
Ambiente	Estrechamente vinculado a los dispositivos informáticos.	Puede ocurrir en el entorno físico, en el entorno digital (*cibernético*) o en ambos de forma acumulativa.

Fuente: El autor, 2026

En resumen, la Ley Carolina Dieckmann garantizó la protección legal del "espacio digital privado" (como un teléfono móvil o una computadora), mientras que la penalización del ciberacoso protege a las personas contra la vigilancia obsesiva y el acoso, tanto en línea como fuera de línea. Ambas medidas trabajan en conjunto para crear un entorno digital más seguro y menos hostil para las víctimas.

2.7 Retos actuales para la protección de la privacidad digital

En la era digital, los desafíos de la privacidad se han vuelto más complejos debido a la intensa circulación de información personal en redes sociales, aplicaciones, plataformas digitales, bases de datos y sistemas automatizados. La recopilación masiva de datos, la falta de transparencia respecto a los fines del procesamiento de datos, la dificultad para obtener un consentimiento verdaderamente informado y el aumento de las filtraciones de datos son algunos de los principales problemas que enfrentan los titulares de los datos.[15]

La vulnerabilidad de los datos personales no solo proviene de ataques técnicos sofisticados, como intrusiones en sistemas o la instalación de programas maliciosos, sino también de prácticas cotidianas como compartir información en exceso, usar contraseñas

[15]MEIRELES, Adriana Veloso. **Privacidad en el siglo XXI: protección de datos, democracia y modelos regulatorios** . *Revista Brasileña de Ciencia Política* . Disponible en: https://www.scielo.br/j/rbcpol/a/my3M8sH3tfpm4WmXhrNcMjK/ . Consultado el 27 de octubre de 2025.

débiles, aceptar automáticamente los términos de uso, exponer imágenes íntimas o familiares, completar formularios en sitios web inseguros e interactuar con enlaces fraudulentos. Estas situaciones crean un entorno propicio para el phishing , el robo de identidad, el fraude electrónico, la intrusión en dispositivos informáticos, la exposición indebida de imágenes y el uso indebido de datos personales.

Proteger la privacidad en las redes sociales y plataformas digitales requiere actuar en múltiples frentes. Es responsabilidad del Estado promulgar la normativa pertinente, supervisar su aplicación y crear organismos capaces de investigar y exigir responsabilidades a los autores de delitos digitales. Al mismo tiempo, los usuarios, las empresas y las instituciones deben adoptar medidas preventivas, estrategias de seguridad de la información y programas de educación digital, ya que la protección de la privacidad no se logra únicamente mediante el castigo una vez producido el daño, sino también reduciendo los riesgos que facilitan la violación de datos personales.

Más allá de la dimensión preventiva, existen importantes desafíos legales, ya que muchos delitos digitales trascienden las fronteras nacionales, lo que dificulta definir la jurisdicción y exigir responsabilidades a los perpetradores. La recopilación de pruebas digitales también presenta obstáculos específicos, dado que los datos pueden ser eliminados, alterados, ocultados o almacenados en servidores ubicados en otros países. A esto se suma el uso de perfiles falsos, mecanismos de anonimización y otras tecnologías de ocultación, que dificultan la identificación de los responsables.

Ante esta realidad, la lucha contra la ciberdelincuencia requiere cooperación institucional e internacional. El Convenio de Budapest sobre la Ciberdelincuencia, promulgado en Brasil mediante el Decreto n.º 11.491/2023, constituye un instrumento relevante para la colaboración entre Estados, especialmente considerando la naturaleza transnacional de muchos delitos cometidos en el entorno digital.[16]

Por lo tanto, la protección de la privacidad digital no puede depender únicamente del enjuiciamiento penal una vez que se ha producido el daño. Es necesario combinar la prevención, la educación digital, la seguridad de la información, la protección de datos personales, la investigación especializada, la cooperación institucional y los mecanismos civiles, administrativos y regulatorios. Solo una respuesta integral puede brindar mayor eficacia en la

[16]BRASIL. **Decreto n.º 11.491, de 12 de abril de 2023.** Por el que se promulga el Convenio sobre la Ciberdelincuencia, firmado en Budapest el 23 de noviembre de 2001.

protección de la intimidad, la vida privada, la autodeterminación informativa y los datos personales en la sociedad digital.

La velocidad es el principal obstáculo en la actualidad. Si bien la ley exige un procedimiento de investigación formal para probar la autoría y la naturaleza del delito, la inteligencia artificial permite al autor borrar sus huellas, cambiar su dirección IP o crear una nueva identidad digital en cuestión de segundos.

Por lo tanto, la protección actual se centra en la defensa proactiva, en lugar de la reactiva (esperar a que se cometa un delito antes de procesarlo). Esto incluye el uso de autenticación multifactor (MFA), claves de seguridad físicas, herramientas de cifrado de extremo a extremo y, sobre todo, formación digital continua para reconocer el fraude psicológico antes de que un dispositivo se vea comprometido.

3 consideraciones finales

Este estudio tuvo como objetivo examinar el derecho a la privacidad en la era digital mediante un análisis de la Ley No. 12.737/2012, conocida como la Ley Carolina Dieckmann, evaluando su importancia, sus límites y su lugar dentro del marco legal brasileño para la protección de la intimidad, la vida privada y los datos personales.

A lo largo de la investigación, se constató que la privacidad ha experimentado una importante transformación conceptual. Inicialmente asociada al derecho a la privacidad, desde una perspectiva más pasiva de protección contra intrusiones indebidas, la privacidad ha adquirido una dimensión más activa en la sociedad digital, relacionada con el control del flujo de información personal. En este contexto, cobra relevancia la noción de autodeterminación informativa, según la cual el individuo debe poder comprender e influir en la recopilación, el uso, el intercambio, el almacenamiento y la circulación de sus datos.

La Ley Carolina Dieckmann representó un hito significativo para el Derecho Penal brasileño, ya que introdujo el delito de acceso no autorizado a dispositivos informáticos en el Código Penal, brindando una respuesta normativa específica a una realidad que hasta entonces no había sido suficientemente abordada por el ordenamiento jurídico. Antes de su promulgación, las conductas que implicaban el acceso no autorizado a computadoras, teléfonos celulares, cuentas digitales y archivos personales se clasificaban frecuentemente como delitos penales tradicionales, que no siempre se ajustaban a la naturaleza de los bienes afectados en el entorno virtual.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 06/10/2026 | Aceptado: 06/13/2026 | Publicación: 06/16/2026

Sin embargo, la suficiencia de la Ley N° 12.737/2012 debe entenderse de forma relativa. Si bien la ley fue esencial como punto de partida para la protección penal de la privacidad digital, no es capaz, por sí sola, de abordar todos los riesgos inherentes a la sociedad de la información. La redacción original del artículo 154-A del Código Penal exigía la violación indebida de un mecanismo de seguridad, lo que generó críticas respecto a la limitación de su aplicación. Con la modificación introducida por la Ley N° 14.155/2021, este requisito dejó de estar expresamente establecido en el texto principal de la disposición, centrando la atención en la intrusión no autorizada en el dispositivo informático de otra persona, asociada al propósito específico de obtener, alterar o destruir datos o información, o instalar vulnerabilidades para obtener una ventaja ilícita.

Este cambio legislativo reforzó la protección penal de la privacidad digital, incluyendo sanciones más severas. Aun así, la protección de la privacidad en el entorno virtual no puede depender exclusivamente del enjuiciamiento penal una vez que se ha producido el daño. La velocidad de difusión de la información, la dificultad para identificar a los perpetradores, la volatilidad de las pruebas digitales y la multiplicidad de formas de violación demuestran la necesidad de una respuesta legal más amplia, preventiva e integral.

En este contexto, el análisis de la Ley Carolina Dieckmann debe articularse con otros instrumentos normativos. La Constitución Federal garantiza la inviolabilidad de la intimidad, la vida privada, el honor y la imagen, e incorpora, mediante la Enmienda Constitucional N° 115/2022, la protección de datos personales como un derecho fundamental autónomo. El Código Civil ofrece instrumentos para la prevención, el cese y la reparación de las violaciones de los derechos de la personalidad. La Carta Brasileña de Derechos de Internet establece principios, garantías, derechos y deberes para el uso de internet en Brasil. La LGPD (Ley General de Protección de Datos de Brasil), por su parte, regula técnicamente el tratamiento de datos personales, imponiendo deberes de seguridad, transparencia, prevención y rendición de cuentas a los responsables del tratamiento de datos.

También se ha observado que las nuevas formas de violación de la privacidad, como el ciberacoso y la divulgación indebida de información personal, aumentan la complejidad del problema. La Ley N° 14.132/2021, al definir el delito de acoso, demuestra que la protección de las personas en el entorno digital no se limita a la defensa de los dispositivos informáticos o los datos almacenados. La protección jurídica debe extenderse también a la libertad, la tranquilidad, la integridad psicológica, la reputación y la seguridad de la víctima, especialmente ante actos reiterados de vigilancia, amenazas, coacción o perturbación perpetrados por medios digitales.

Por lo tanto, se puede concluir que la Ley Carolina Dieckmann sigue siendo un instrumento relevante para la protección penal de la privacidad digital, pero su efectividad depende de una interpretación actualizada y su integración con el marco constitucional, civil, administrativo y normativo para la protección del individuo. La privacidad en la era digital no se protege mediante una sola norma, sino mediante un ecosistema jurídico compuesto por normas penales, civiles, constitucionales y de protección de datos personales.

Por lo tanto, proteger la privacidad digital requiere no solo castigar a los responsables de los ataques informáticos, sino también educación digital, seguridad de la información, prevención de riesgos, conservación adecuada de las pruebas, responsabilidad civil y administrativa, y el fortalecimiento de la cultura de protección de datos personales. El desafío actual reside en encontrar el equilibrio entre la innovación tecnológica, la libertad de uso de internet y la protección de la dignidad humana en el ciberespacio.

Finalmente, se recomienda que futuros estudios profundicen en el impacto de la inteligencia artificial, la recopilación masiva de datos, las decisiones automatizadas y las nuevas formas de vigilancia digital sobre la privacidad y la autodeterminación informativa. La constante evolución tecnológica impone al derecho el deber de actualizarse permanentemente, de modo que la protección de la intimidad, la vida privada y los datos personales siga siendo efectiva frente a las nuevas formas de violación en el entorno digital.

Referencias

ALMEIDA, Karen Rosa de. **Ciberacoso : del marco actual a la necesidad de protección específica: un análisis a la luz del ordenamiento jurídico brasileño y el derecho comparado** . Disponible en: <https://periodicos.ufba.br/index.php/rppgd/article/download/36359/24988/175050> Consultado el 25 de octubre de 2025.

ASSUNÇÃO, Ana Paula Souza. **Ciberdelitos** . Disponible en: <http://repositorio.aee.edu.br/bitstream/aee/538/1/Monografia%20-%20Ana%20Paula%20Souza.pdf> Consultado el 22 de octubre de 2025.

BARATTA, Alessandro. **Criminología crítica y crítica del derecho penal: Introducción a la sociología del derecho penal** . 3.ª ed. Río de Janeiro: Revan, 2002.

BIONI, Bruno. **Responsabilidad civil en la protección de datos personales: construyendo puentes entre la Ley General de Protección de Datos Personales y el Código de Protección del Consumidor** . civilistica.com, vol. 9, n.º 3, págs. 1-23, 22 de diciembre de 2020.

BISPO, Adrielle da Silva. **Delitos cibernéticos: la ineficacia de la ley Carolina Dieckmann en la práctica de los delitos virtuales** . Disponible en: < https://periodi-

corease.pro.br/rease/article/download/12291/5727/23272>. Consultado el 28 de octubre de 2025.

BRASIL, 2018. **Ley N° 13.709, del 14 de agosto de 2018.** Disponible en: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Consultado el 2 de octubre de 2025.

BRASIL. **Ley N° 8.078, del 11 de septiembre de 1990.** Disponible en: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm> Consultado el: 20 de octubre de 2025.

BRASIL. **Decreto-Ley N° 3.914, del 9 de diciembre de 1941.** Disponible en: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm> Consultado el 17 de octubre de 2025.

BRASIL. Ley N° 14.132, del 31 de marzo de 2021. **Añade el artículo 147-A al Decreto Ley N° 2.848, del 7 de diciembre de 1940 (Código Penal), para tipificar el delito de acoso; y deroga el artículo 65 del Decreto Ley N° 3.688, del 3 de octubre de 1941 (Ley de Delitos Penales)** . Disponible en: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm> Consultado el 12 de junio de 2026.

BRASIL. **Ley N° 12.737, del 30 de noviembre de 2012.** Establece la penalización de los delitos informáticos. Modifica el Decreto-Ley N° 2.848, del 7 de diciembre de 1940 - Código Penal; y dispone otras medidas. Brasilia, DF. 3 de diciembre de 2012. Disponible en: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12737.htm > Consultado el 24 de octubre de 2025.

COLHADO, Junyor Gomes. **Concepto de delito en el Derecho Penal Brasileño** . Disponible en: <https://jus.com.br/artigos/47517/conceito-de-crime-no-direito-penal-brasileiro> Consultado el: 7 de marzo de 2025.

COPETTI, Rafael; MIRANDA, Marcel Andreata De. et al. **Autodeterminación informacional y protección de datos: un análisis crítico de la jurisprudencia brasileña. Derecho, gobernanza y nuevas tecnologías** . Florianópolis: CONPEDI, 2015. Disponible en: < http://www.egov.ufsc.br/portal/sites/default/files/j6023guzncw4in57.pdf > Consultado el 10 de junio de 2026.

DENNY, Danielle Mendes Thame et al., **Derecho internacional en la era del populismo digital** . Disponible en: <https://revista.internetlab.org.br/direito-internacional-na-erado-populismo-digital/> Consultado el 29 de octubre de 2025.

DONEDA, Danilo. **De la privacidad a la protección de datos personales** . São Paulo: Thomson Reuters, 2019.

FERNANDES, Aloir de Araújo. **Delitos en internet, la ley Carolina Dieckmann y sus defectos** . Disponible en: <https://ri.unipac.br/repositorio/wp-content/uploads/tainacanitems/282/137736/ALOIR-DE-ARAUJO-FERNANDES-CRIMES-NA-INTERNET-LEICAROLINA-DIECKMANN-DIREITO-2015.pdf> Consultado el 30 de octubre de 2025.

FONTES, Jose Igor Alves. **Datos personales digitales y su tratamiento en el ordenamiento jurídico brasileño** . Tesis de grado (Derecho) - UFRN. Natal/RN: Biblioteca Sectorial CCS, 2018. Disponible en: < https://monografias.ufrn.br/jspui/bitstream/123456789/7356/1/Dados%20Pessoais_Fontes_2018.pdf >. Consultado el 5 de junio de 2026.

HINTZBERGEN, Jule. et al. **Fundamentos de la seguridad de la información: basados en ISO 27001 e ISO 27002.** Traducido por Alan de Sá. Río de Janeiro: Brasport , 2018.

MACHADO, Rafael Lopes Kassem. CIBERDELITOS, INVASIÓN DE LA PRIVACIDAD Y LA EFICACIA DE LA RESPUESTA ESTATAL: los impactos de la Ley 12.737/2012 – Ley Carolina Dieckmann y el Reglamento General de Protección de Datos en la lucha contra los ciberdelitos de invasión de la privacidad. Disponible en: <https://projecaociencia.com.br/index.php/Projecao2/article/download/1798/1444> Consultado el 20 de octubre de 2025.

MAIA, Daniel. **Criminalización del** acoso **en Brasil: análisis del artículo 147-** A **del código penal a la luz del derecho a la privacidad** . Disponible en: <https://repositorio.ufc.br/handle/riufc/73074 >. Consultado el 11 de junio de 2026.

MASSON, Cléber. **Derecho Penal Esbozado** . Editora Método, São Paulo, 2009.

MEIRELES, Adriana **Veloso. Privacidad en el siglo XXI: protección de datos, democracia y modelos regulatorios** . Disponible en: <https://www.scielo.br/j/rbcpol/a/my3M8sH3tfpm4WmXhrNcMjK/ > Consultado el 27 de octubre de 2025.

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

MUÉS, Gustavo Brandão Koury. **DELITOS VIRTUALES: Un análisis de la adecuación del derecho penal brasileño** . Disponible en: <https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf> Consultado el 19 de octubre de 2025.

NETTO, Thaís. **Seguridad de la información: Mecanismos de protección dentro de las organizaciones** . Disponible en: <https://direitoreal.com.br/artigos/segurancadainformacao-mecanismos-de-protecao-dentro-das-organizacoes> Consultado el: 22 de octubre de 2025.

OTOBONI, Gustavo Henrique dos Santos **. Ciberdelitos: phishing . 2019.** Disponible en: <https://ambitojuridico.com.br/edicoes/revista191/crimescibernetico-phishing/>. Consultado el 26 de octubre de 2025.

PEIXOTO, Andréa Stefani. **Ley de Protección de Datos: ¡entiéndala en 13** puntos **!** Disponible en: <https://www.politize.com.br/lei-de-protecao-de-dados/ > 2020 , pág. 43. Consultado el 29 de octubre de 2025.

PINHEIRO, Patricia Peck. **Derecho Digital** . 7ª edición. São Paulo: Saraiva, 2021.

ROSA, Fabricio. **Delitos informáticos** . Campinas: Librero , 2002.
SCHIMIDT, Guilherme. **Delitos cibernéticos** . Disponible en: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Consultado el 26 de octubre de 2025.

SILVA, Márcio Ferreira da. **Efectividad de la Ley Carolina Dieckman** . Disponible en: <http://repositorio.aee.edu.br/bitstream/aee/17530/1/2017%20-TCC%20-%20MARCIO%20FERREIRA%20DA%20SILVA.pdf> Consultado el 30 de octubre de 2025.

SILVA, Patrícia Santos da. **Derecho cibernético y delincuencia: un análisis de la jurisdicción según la ubicación en el enjuiciamiento de casos penales** . Brasilia: Vestnik , 2019.

SOUZA, Marcela Tavares et al. Revisión integradora: qué es y cómo hacerla. **Revista Einstein** . vol. 8, págs. 102-106, 2010. Disponible en: <http://www.scielo.br/pdf/eins/v8n1/pt_1679-4508-eins-8-1-0102.pdf.> Consultado el: 20 de octubre de 2025.

STEFAM, André. **Derecho Penal: Parte General** (Artículos 1 al 120). São Paulo: Saraiva Educação, 2018.

TEIXEIRA, Tarcísio. **Derecho Digital y Proceso Electrónico** . 5ª edición. São Paulo: Saraiva, 2020.

VIEIRA, Waleska Duque Estrada. Privacidad en el entorno cibernético: Un derecho fundamental del usuario. Revista **da ESMESC , v. 24, n. 30, p.** 197-217 , 2017. Disponible en: https://revista.esmesc.org.br/re/article/view/167 . Consultado el 10 de mayo de 2026. DOI : https://doi.org/10.14295/revistadaesmesc.v24i30.p197