LUMEN ET VIRTUS
ISSN: 2177-2789

A EFICÁCIA DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) NO COMBATE AOS CRIMES CIBERNÉTICOS E NA PROTEÇÃO DA PRIVACIDADE DOS USUÁRIOS

THE EFFECTIVENESS OF THE GENERAL DATA PROTECTION LAW (LGPD) IN COMBATING CYBERCRIMES AND PROTECTING USER PRIVACY

LA EFICACIA DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) EN LA LUCHA CONTRA LOS CIBERDELITOS Y LA PROTECCIÓN DE LA PRIVACIDAD DE LOS USUARIOS

https://doi.org/10.56238/levv17n58-081

Data de submissão: 01/03/2026 **Data de publicação:** 30/03/2026

Thainara de Jesus Rodrigues
Graduanda em Direito
Instituição: Faculdade de Tecnologia, Filosofia e Ciências Humanas Gamaliel
E- mail: thainara.rodrigues@faculdadegamaliel.com.br

Antônio Carlos Pantoja Freire
Professor Mestre Orientador da disciplina de Trabalho de Conclusão de Curso (TCC)
E-mail: antonio.freire@faculdadegamaliel.com.br

RESUMO

O presente trabalho busca abordar que, com a evolução da sociedade e os avanços tecnológicos, houve também um aumento significativo dos crimes cibernéticos, o que acaba representando um risco à segurança de indivíduos e instituições. Diante desse cenário, tornou-se necessária a criação de leis que pudessem prever e tipificar essas condutas. Para que esses crimes não ficassem impunes, e em decorrência do grande aumento de casos de delitos virtuais, foi necessário o desenvolvimento de legislações específicas voltadas para essa realidade. Nesse contexto, em 2012 foi criada a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que promoveu alterações no Código Penal brasileiro com o objetivo de tipificar condutas relacionadas à invasão de dispositivos informáticos. Além disso, também foi sancionada a Lei Geral de Proteção de Dados (LGPD) em 2018, que estabelece normas para o tratamento de dados pessoais e prevê responsabilidades para empresas e instituições que não adotam medidas adequadas de segurança para prevenir ataques cibernéticos e a violação de informações. Dessa forma, a legislação brasileira passou a buscar maior proteção aos dados e à privacidade no ambiente digital.

Palavras-chave: Crimes Cibernéticos. Roubo de Dados. Proteção de Dados Pessoais.

ABSTRACT

This paper aims to address the fact that, with the evolution of society and technological advancements, there has been a significant increase in cybercrime, which represents a risk to the security of individuals and institutions. Given this scenario, it became necessary to create laws capable of addressing and classifying such conduct. In order to prevent these crimes from going unpunished, and due to the considerable increase in cases of virtual offenses, it was necessary to develop specific legislation aimed

at this reality. In this context, Law No. 12.737/2012, known as the Carolina Dieckmann Law, was enacted in 2012, amending the Brazilian Penal Code to criminalize conduct related to the invasion of computer devices. Furthermore, the General Data Protection Law (LGPD) was enacted in 2018, establishing rules for the processing of personal data and defining responsibilities for companies and institutions that fail to adopt adequate security measures to prevent cyberattacks and data breaches. Therefore, Brazilian legislation has sought to provide greater protection for data and privacy in the digital environment.

Keywords: Cybercrime. Data Theft. Personal Data Protection.

RESUMEN

Este artículo aborda el hecho de que, con la evolución de la sociedad y los avances tecnológicos, también se ha producido un aumento significativo de los ciberdelitos, lo que representa un riesgo para la seguridad de las personas e instituciones. Ante este panorama, se hizo necesario crear leyes que pudieran prever y clasificar estas conductas. Para evitar que estos delitos queden impunes, y debido al gran aumento de casos de delitos virtuales, fue necesario desarrollar una legislación específica centrada en esta realidad. En este contexto, en 2012 se promulgó la Ley N° 12.737/2012, conocida como Ley Carolina Dieckmann, que modificó el Código Penal brasileño para clasificar las conductas relacionadas con la intrusión en dispositivos informáticos. Asimismo, en 2018 se promulgó la Ley General de Protección de Datos (LGPD), que establece normas para el tratamiento de datos personales y determina las responsabilidades de las empresas e instituciones que no adopten medidas de seguridad adecuadas para prevenir los ciberataques y la violación de la información. De esta manera, la legislación brasileña ha comenzado a buscar una mayor protección de los datos y la privacidad en el entorno digital.

Palabras clave: Delitos Cibernéticos. Robo de Datos. Protección de Datos Personales.

1 INTRODUÇÃO

O presente trabalho tem por tema os crimes cibernéticos. Trata-se de um tipo de delito no qual os criminosos utilizam-se da internet para praticar diversas infrações, muitas vezes com a finalidade de enganar as vítimas e obter vantagem indevida. Apesar de ser um tema amplo, o foco desta pesquisa é o roubo de dados, entendido como a aquisição não autorizada de informações pessoais ou até mesmo confidenciais.

O ordenamento jurídico brasileiro dispõe de normas que regulamentam a proteção de dados pessoais, como a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, bem como o Código Penal, Decreto-Lei nº 2.848/1940, que criminaliza condutas relacionadas ao roubo de dados.

Os crimes cibernéticos vêm ganhando destaque especialmente em razão do papel revolucionário da internet. Durante a pandemia da COVID-19, a dependência das tecnologias digitais aumentou significativamente, devido ao isolamento social, que impulsionou o trabalho remoto, os estudos on-line, o comércio eletrônico e novas formas de interação social.

Nesse contexto, diversas práticas criminosas se expandiram, como golpes, roubo de dados, propagação de pornografia infantil, fraudes financeiras, ransomware, entre outras. Muitos criminosos acreditam que, por estarem atrás de uma tela, permanecerão impunes. Surge, então, o questionamento sobre a eficácia da legislação brasileira no combate ao roubo de dados: será que o ordenamento jurídico vigente é suficiente para enfrentar essas novas modalidades de crimes virtuais?

O estudo possui grande relevância social, considerando que, juntamente com os avanços tecnológicos, surgem também novas práticas delitivas no meio virtual, especialmente diante do uso crescente da internet. Assim, torna-se essencial analisar se as legislações atuais são capazes de prevenir e punir os crimes cibernéticos.

O objetivo deste estudo é analisar os crimes cibernéticos, com ênfase no roubo de dados, demonstrando que a legislação atual, em alguns aspectos, já não consegue acompanhar a rápida evolução das práticas criminosas digitais. Serão examinadas a Lei nº 13.709/2018 (LGPD), que visa resguardar os direitos fundamentais de liberdade e privacidade, bem como o Código Penal, Decreto-Lei nº 2.848/1940, e demais legislações pertinentes.

A pesquisa será desenvolvida por meio de revisão de literatura, buscando entender o que já se discute a respeito do tema de crimes cibernéticos, a fim de proporcionar uma compreensão mais aprofundada do tema.

2 CRIMES CIBERNÉTICOS

2.1 HISTÓRIA DA INTERNET

A internet que usamos nos dias atuais, já teve outra finalidade bem diferente, isso porque a internet nasceu em 1960, em decorrência da Guerra Fria, entre uma disputa dos Estados Unidos e a

União Soviética, e a principal finalidade da internet era para fins militares, permitindo o compartilhamento de pesquisas e recursos. Conforme expõe: (LINS, 2010, p. 13).

> A rede, no entanto, nasceu bem antes, nos anos sessenta, como resultado de um esforço do sistema de defesa dos EUA para dotar a comunidade acadêmica e militar de uma rede de comunicações que pudesse sobreviver a um ataque nuclear. A ideia era bastante trivial: ao contrário de outras redes existentes, controladas de modo centralizado, seria criada uma rede em que cada equipamento seria relativamente autônomo e a comunicação se daria de modo distribuído. Com uma organização desse tipo, pedaços da rede que não fossem afetados por uma agressão poderiam manter-se em operação. Esse projeto, que recebeu o nome de ARPANET, foi o embrião de uma rede mundial, uma "rede de redes", a Internet que hoje conhecemos.

Em 1969, tivemos a primeira mensagem enviada, que foi transmitida do computador da Universidade da Califórnia para o computador de Stanford. Alguns anos depois, a internet passou a ser utilizada para fins comerciais e, consequentemente, começou a ser usada por todos, mudando a forma de comunicação das pessoas. No Brasil, a internet só chegou no ano de 1988, por meio de comunidades acadêmicas do Rio de Janeiro e de São Paulo. Depois, a internet deixou de ser utilizada somente para fins acadêmicos e passou a ser usada também para fins comerciais. (BRASIL ESCOLA, 2008).

Assim, com a evolução da internet que passou a ser acessível para todos, mas que existem dois lados, o que trouxe grandes benefícios, e que também tem seus prejuízos, pois, com o avanço das ciências eletrônicas surgem novas modalidades de crimes, os chamados crimes cibernéticos, porque ao invés de usarem a internet para coisas do seu dia a dia, fazem totalmente o contrário. (COLARES, 2002).

3 CONCEITO DE CRIMES CIBERNÉTICOS

O crime cibernético consiste no ato de utilizar um computador ou fazer uso da tecnologia para a prática de crimes virtuais. Trata-se de uma conduta ilícita, uma vez que esse tipo de delito está relacionado à violação de direitos fundamentais, ou seja, todas as atividades criminosas que envolvem o uso da tecnologia e do computador configuram crime cibernético. (ALEXANDRE JUNIOR, 2019).

Sabe-se que os crimes cibernéticos são caracterizados pela prática de condutas ilícitas no meio virtual, no qual há uma grande diversidade de atividades criminosas. Para a execução dessas condutas, faz-se necessário o uso de aparelhos eletrônicos com acesso à internet. (GUIMARÃES, 2024).

Desse modo, é importante mencionar Rosa (2006, p. 53) que expõem o conceito da internet tal como:

> A conduta atenta contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela complicação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenamento de dados, ou seja, ainda, na forma mais rudimentar; 2. O,, Crime de Informática" é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o "Crime de informática" pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetra-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertence à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

A Organização das Nações Unidas (ONU) nos ensina o seu próprio conceito sobre os crimes cibernéticos, e diz o seguinte:

> Os crimes cibernéticos são uma forma transnacional em expansão. Sua natureza complexa de crime que ocorre no ciberespaço, sem fronteiras, é agravada pelo crescente envolvimento de grupos do crime organizado.

Conforme Damásio (2016, p. 48), "Crime informático é um fenômeno inerente às transformações tecnológicas que a sociedade experimenta e que influenciam diretamente no Direito Penal". Segundo Sérgio Marcos Roque (2011, p. 25), o conceito de crime cibernético é "toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material".

Portanto, compreende-se que os crimes cibernéticos são praticados no meio virtual e existem várias doutrinas que os classificam no geral como qualquer atividade que faça uso da na internet ou de qualquer meio de tecnologia para a prática de condutas delitivas, é considerada crimes cibernéticos.

4 ROUBO DE DADOS NO AMBIENTE VIRTUAL

4.1 CONCEITO DE DADOS PESSOAIS E DADOS SENSÍVEIS

Diante de uma sociedade cada vez mais informatizada, Danilo Doneda ensina que os dados pessoais possuem grande relevância para as relações sociais, pois o desenvolvimento tecnológico contribuiu para a organização e o armazenamento de dados. Nesse sentido, o autor expõe que "a novidade fundamental introduzida pelos computadores é a transformação de informação dispersa em informação organizada" (DONEDA, 2011).

Desse modo, entende-se que os dados pessoais são um conjunto de informações de cada indivíduo e que eles guardam toda e qualquer informação sobre nós. Os dados pessoais existem muito antes da evolução eletrônica e até mesmo antes do surgimento do CPF. Acontece que, antes, havia outras formas de guardar informações sobre determinada pessoa, como, por exemplo, telegramas,

cartas ou fotos, até chegarmos à era da internet, que passou a contar com novas formas de armazenar nossas informações em sistemas (SOUZA, 2016).

Assim, vale ressaltar que, nos dias atuais, é muito fácil reunir, analisar e até mesmo vender informações pessoais. Pois hoje não existe forma de uma pessoa viver em sociedade sem ter seus dados pessoais em algum banco de dados, conforme explica Doneda (2006).

> Hoje, a exposição indesejada de uma pessoa aos olhos alheios se dá com maior frequência através da divulgação de seus dados pessoais do que pela intrusão em sua habitação, pela divulgação de notícias a seu respeito na imprensa, pela violação de sua correspondência (...).

É obvio que com esse avanço em relação aos dados pessoais, ele tem seus pontos positivos e os negativos. Mas nós precisamos entender o que são dados pessoais e os dados sensíveis.

A Lei Geral de Proteção de Dados (LGPD) estabelece uma distinção entre dados pessoais e dados pessoais sensíveis. Os dados pessoais correspondem a todas as informações capazes de identificar ou tornar identificável uma pessoa natural. Por sua vez, os dados pessoais sensíveis referem-se às informações que, caso sejam divulgadas ou utilizadas de forma inadequada, podem gerar situações de discriminação ou violação de direitos fundamentais. (MULHOLLAND, 2018).

> Para fins de regulação das atividades de tratamento de dados, a Lei Geral de Proteção de Dados Brasileira (LGPD) categoriza e tutela de forma diferenciada os dados pessoais e os dados pessoais sensíveis. Para os fins da LGPD, dado pessoal é composto por informações relacionadas a pessoa natural identificada ou identificável (artigo 5º, I) e dado pessoal sensível se refere à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II).

BRASIL. Lei nº 13.709/2018, art. 5º:

> I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II – dado pessoal sensível: dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

5 FORMAS DE OCORRÊNCIA DO ROUBO DE DADOS

No mundo digital, existem diversas formas de roubo de dados, e cada uma dessas modalidades possui métodos e características próprios que facilitam a subtração de dados pessoais, como dados sensíveis ou até mesmo informações confidenciais. Destaca-se que os crimes cibernéticos vêm aumentando em decorrência do crescimento do uso da tecnologia na sociedade moderna (Marques, 2023).

> Os dados roubados podem incluir informações pessoais, como nomes, endereços, números de telefone, informações financeiras, senhas e até mesmo dados de saúde. O objetivo dos criminosos pode variar desde o roubo de identidade até a extorsão, venda de informações no mercado negro ou a realização de fraude financeiras.

Dessa forma, ao longo dos anos, os crimes cibernéticos tornaram-se mais sofisticados, surgindo diversas modalidades de delitos, como malware, ransomware, ameaças persistentes avançadas (APTs), negação de serviço e phishing. Atualmente, com o avanço da inteligência artificial (IA), também surgem golpes como o *deepfake*, conforme aponta a Microsoft (2023).

O phishing é uma modalidade que vem se destacando significativamente, pois os criminosos conseguem ludibriar suas vítimas ao se passarem por empresas confiáveis, por meio de mensagens falsas com a finalidade de obter informações pessoais, como números de contas ou senhas. Já o malware consiste, basicamente, em um software malicioso criado especialmente para o roubo de dados, espionagem ou até mesmo para danificar sistemas (Marques, 2023).

6 IMPACTOS DO ROUBO DE DADOS PARA INDIVÍDUOS E INSTITUIÇÕES

A Lei Geral de Proteção de Dados foi criada pensando na proteção de dados pessoais e nas consequências que os ataques cibernéticos podem causar às pessoas e às empresas. Pois, devido ao aumento de casos de roubo de dados, traz grandes impactos que não são apenas financeiros, mas que acabam afetando a vida dessas vítimas. Conforme ensina Fagundes (2023).

> É importante também abordar os impactos psicológicos e emocionais que as vítimas enfrentam após terem suas informações roubadas. A sociedade deve garantir que haja apoio e recursos adequados para ajudar essas pessoas a lidar com as consequências do roubo de dados, bem como para prevenir futuras violações de segurança e proteger a privacidade dos cidadãos.

Assim, também é necessário destacar que, para cair em golpes, muitas vezes nem é preciso que a vítima compartilhe suas informações pessoais com esses criminosos. Conforme expõe Rodrigues (2024).

> Quando ocorre um data breach, informações pessoais, financeiras, médicas ou comerciais, podem ser comprometidas e potencialmente utilizadas de maneira indevida por indivíduos mal-intencionados. As violações de dados podem ter sérias consequências, incluindo danos à reputação da empresa, perda de confiança dos clientes, multas regulatórias e prejuízos financeiros. Portanto, é fundamental que as organizações implementem medidas de segurança robustas para proteger os dados confidenciais e estejam preparadas para responder de maneira eficaz em caso de violação de dados.

Portanto, diante de casos de roubo de dados, a empresa acaba perdendo sua credibilidade aos olhos de seus clientes, que passam a não confiar nas medidas de segurança que a instituição adota. Como a empresa também precisa seguir várias determinações impostas pela Lei Geral de Proteção de Dados (LGPD), que garante a proteção de informações.

7 A LEGISLAÇÃO BRASILEIRA FRENTE AO ROUBO DE DADOS

7.1 LEI N° 12.737/2012 (LEI CAROLINA DIECKMANN)

A lei que conhecemos como Carolina Dieckmann, foi publicada após o caso envolvendo a atriz brasileira que teve suas fotos íntimas vazadas na internet. Essa norma tem como foco tipificar invasão de dispositivos informáticos e trazer segurança para os usuários de meios eletrônicos. Conforme Monteiro (2022, p.1):

> A lei trouxe uma ferramenta a mais para punição dos crimes informáticos, porque antes [mecanismo] que tínhamos tratava-os apenas como atos preparatórios. Antes, só o fato de você ter acesso ao dispositivo não era considerado crime. Com o advento da lei, isso passou a ser crime.

Além disso, Monteiro expõe como ocorreu a criação da Lei Carolina Dieckmann e destaca sua principal finalidade, que consiste no combate aos crimes informáticos. O caso teve início quando um hacker invadiu o computador pessoal da atriz e obteve acesso a fotos de natureza íntima. Posteriormente, passou a chantagear a vítima, exigindo o valor de R$ 10.000,00 (dez mil reais). Diante da recusa da artista em efetuar o pagamento, o hacker divulgou as imagens na internet. O episódio gerou ampla discussão e grande repercussão na mídia, culminando na promulgação da Lei Carolina Dieckmann (Lei nº 12.737/2012).

Assim, também é importante destacar que, antes da criação dessa lei, tais delitos já ocorriam, não havendo legislação específica capaz de punir os responsáveis e proteger as vítimas. Como nos ensina Cardoso (2024).

> Antes da Lei Carolina Dieckmann, não havia uma legislação específica para crimes cibernéticos no Brasil. As pessoas que cometiam crimes digitais eram punidas com base em outras leis, como a Lei de Propriedade Intelectual, a Lei de Direitos Autorais e o Código Penal. Essas leis não eram suficientes para lidar com os novos tipos de crimes que surgiram com a popularização da internet e das tecnologias digitais.

Portanto, Cardoso nos ensina que, à época do ocorrido, vivia-se um cenário de grande fragilidade em relação à segurança digital e que, pela ausência de norma específica, não havia meios adequados para punir o responsável pelo crime cometido contra a artista.

Nesse contexto, o Código Penal, em seu Decreto-Lei nº 2.848/1940, foi alterado pela Lei nº 12.737/2012, que veio para tipificar os crimes cibernéticos, mediante o seu art. 154-A.

> Art. 154-A. Invadir disposto 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 dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" (BRRASIL, 2012, s.p).

Ou seja, a Lei Carolina Dieckmann veio para resguardar o direito de pessoas que têm informações pessoais subtraídas de seus aparelhos eletrônicos. Essa lei veio para garantir que criminosos sejam punidos de acordo com seus delitos.

8 LEI GERAL DE PROTEÇÃO DE DADOS (LEI N° 13.709/2018)

No Brasil, foi sancionada a Lei nº 13.709/2018. Com a constante crescente da utilização de dados pessoais em um mundo globalizado, fez-se necessário criar uma lei que pudesse regular a utilização dessas informações, tanto por pessoas físicas quanto jurídicas, no meio público e privado também. Conforme expõe o artigo 1º dessa lei.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Dessa forma, a lei destaca que os dados pessoais fazem parte da identidade e dignidade da pessoa, e o objetivo da LGPD é criar um ambiente em que as pessoas possam desenvolver suas atividades cotidianas e viver em sociedade sem medo de ter suas informações manipuladas no meio digital.

Em seu art. 2º a lei exibe os principais fundamentos que são adotados como métodos para a resguardar direitos fundamentais.

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A LGPD foi criada com a finalidade de garantir que as pessoas tenham direto de controlas seus dados pessoais, fazendo com que as pessoas saibam em que suas informações estão sendo usadas e de que forma. O jurista brasileiro Danilo Doneda, expressa o seguinte sobre a LGPD:

> A LGPD foi um marco necessário para assegurar que o tratamento de dados pessoais no Brasil ocorra em um ambiente que respeite os direitos fundamentais e a dignidade da pessoa humana, garantindo que os titulares possam ter controle sobre suas informações.

Mas também é necessário adotar algumas medidas de segurança, que possam proteger os dados pessoais contra qualquer forma de acesso indevido. Nesse sentido, após a criação da lei LGPD, em caso de vazamento de dados, as empresas têm algumas regras a seguir de acordo com o que a lei exige. Conforme o artigo 46 da lei.

> Art.46. Os agentes de tratamentos devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizado e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Portanto, vale ressaltar que a LGPD é crucial para o combate de crimes cibernéticos, isso porque ela no trás regras e responsabilidades em proteger informações pessoais e sessar os riscos causados por esses delitos.

9 A LEGISLAÇÃO PENAL BRASILEIRA

O Código Penal brasileiro é regido pela Decreto-Lei nº 2.848/1940, e ele é responsável por estabelecer regras e aplicar sanções no âmbito dos crimes que são cometidos no meio social, pois é uma forma de punir ou estabelecer consequências para determinadas ações que são consideradas crimes. Diante da constante evolução da sociedade e de meios tecnológicos, o Código Penal não conseguia, por si só, legislar sobre questões que vêm sendo abordadas à medida que vão surgindo novas modalidades de crimes. O que significa dizer que antes ele não previa essas nuances dos crimes digitais.

Desse modo, surge então, a necessidade da criação de leis que pudessem prever esses delitos. De acordo com (QUEIROZ, 2021, P. 20).

> O Direito é a única forma de controle que pode conter o avanço da criminalidade no mundo virtual, de todos os sistemas de controle social, também é o único que exerce coercitividade, sancionando e punindo as condutas havidas por ilícitas.

Além disso, os crimes cibernéticos são crimes que acontecem a todo momento em algum lugar do mundo, em decorrência da constante evolução da tecnologia, que nos proporciona uma vasta facilidade de viver em sociedade. Com essa evolução, surgem diferentes formas de crimes; com isso, se faz necessário que o Direito Penal venha buscar maneiras de amenizar e penalizar esses tipos de delitos.

Em decorrência dessa necessidade foram criadas leis que pudessem criminalizar esses tipos de delitos, como a Lei Carolina Dieckmann, que veio para tipificar “invasão de dispositivos eletrônicos” bem como a como “interrupção ou perturbação de serviços telegráfico, telefônico, informático,

telemático ou de informação de utilidade pública". A Lei Geral de Proteção de Dados (LGPD), que implementou medidas de segurança contra o roubo de dados pessoais.

Dessa forma, podemos destacar que o nosso Código Penal vem ao longo dos anos tentando acompanhar a evolução da sociedade, com o intuito de proteger e garantir os direitos de indivíduos e empresas que sofram ataques cibernéticos.

10 EFETIVIDADE DA LEGISLAÇÃO BRASILEIRA NO COMBATE AOS CRIMES CIBERNÉTICOS

10.1 DESAFIOS NA INVESTIGAÇÃO E PUNIÇÃO DOS CRIMES CIBERNÉTICOS

O Brasil avançou significativamente na criação de leis específicas para o combate aos crimes cibernéticos. Contudo, ainda enfrenta obstáculos quanto à efetiva aplicação dessas normas, uma vez que os criminosos virtuais se aperfeiçoam à medida que a tecnologia evolui. Além disso, os investigadores precisam lidar com a insuficiência de recursos, o que acaba dificultando a obtenção de provas contra esses agentes. Nesse sentido, expõe (SOARES, 2018)

> A tecnologia da informática é detentora de grande complexidade e dinamismo sem igual, o que faz com que os órgãos investigativos e judiciários não estejam adequadamente preparados para lidar com esta nova criminalidade e a cada uma de suas repentinas mudanças. Não muito dificilmente serão encontrados agentes públicos sem qualquer conhecimento sobre as tecnologias e das informações necessárias para uma melhor prestação da proteção estatal aos cidadãos nos órgãos responsáveis pela persecução penal.

O Brasil enfrenta diversos obstáculos referentes à investigação de crimes virtuais, o que, consequentemente, acaba aumentando o índice de impunidade. Um dos principais fatores que interferem na investigação pelas autoridades competentes é a dificuldade de rastrear os criminosos, uma vez que o anonimato é uma das características que a internet pode proporcionar. Nesse sentido, Lopes (2021) afirma que é relativamente fácil para os criminosos cometerem seus delitos, pois a internet pode favorecer o anonimato, ou seja, uma forma de praticar crimes sem expor a própria identidade. Além disso, os criminosos utilizam softwares para navegar na internet de forma anônima, o que dificulta a identificação dos autores e a produção de provas.

Os criminosos podem cometer seus crimes em qualquer lugar do mundo, bastando ter acesso à internet, o que levanta um ponto importante: o desafio de melhorar a cooperação entre as autoridades brasileiras e internacionais para reunir recursos e tecnologias voltados ao combate desses delitos. Conforme nos ensina (Ferreira, 2020).

> A ausência de mecanismos céleres de cooperação entre autoridades nacionais e estrangeiras dificulta o acesso a informações fundamentais para a investigação, como registros de conexões e conteúdos hospedados em servidores estrangeiros. A ratificação da Convenção de Budapeste pelo Brasil representa um avanço nesse sentido, mas ainda há entraves burocráticos e jurídicos que impactam a efetividade da colaboração no âmbito global dos países.

Desse modo, Souza e Lima (2022) afirmam que existe uma série de fatores que influenciam na investigação de crimes virtuais, pois os órgãos brasileiros necessitam não apenas de profissionais qualificados para exercer essa função, como também de softwares especializados e equipamentos atualizados. Todos esses elementos fazem diferença no momento em que as autoridades realizam as investigações.

11 CONSIDERAÇÕES FINAIS

Este estudo tem como finalidade realizar uma análise acerca dos crimes cibernéticos, com enfoque no roubo de dados, buscando demonstrar os impactos que esse tipo de delito pode causar para indivíduos e instituições, bem como compreender de que forma o ordenamento jurídico brasileiro busca soluções para tratar desses casos.

A internet vem avançando significativamente ao longo dos anos, o que aumenta cada vez mais o número de pessoas conectadas a ela. Embora tenha trazido inúmeros benefícios para a sociedade, esses avanços também contribuíram para o surgimento de novas formas de criminalidade, como o roubo de dados. À medida que a tecnologia evolui, os crimes virtuais também se tornam mais frequentes e sofisticados, podendo causar diversos prejuízos tanto para pessoas físicas quanto para instituições.

Desse modo, percebe-se que a legislação brasileira tem buscado acompanhar essas mudanças, criando leis que possam prever esses crimes e punir os responsáveis, como forma de reduzir a prática de delitos no ambiente digital. Nesse contexto, foi criada a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que surgiu com o objetivo de proteger informações e responsabilizar condutas criminosas praticadas no meio virtual.

Portanto, fica evidente que a legislação brasileira já apresentou avanços significativos no que diz respeito à criação de normas voltadas à repressão dos delitos cometidos no ambiente digital. No entanto, ainda se faz necessário que o ordenamento jurídico continue evoluindo, acompanhando as transformações tecnológicas e os anseios da sociedade.

REFERÊNCIAS

LINS, Bernardo Felipe Estellita. **A evolução da internet: uma perspectiva histórica.** Disponível em: <http://www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf>. Acesso em: 04 de fevereiro de 2026.

SILVA, Daniel Neves. "**História da internet**"; *Brasil Escola*. Disponível em: https://brasilescola.uol.com.br/informatica/internet.htm. Acesso em 04 de fevereiro de 2026.

COLARES, Rodrigo Guimarães. *Cibercrimes: os crimes na era da informática*. Consultor Jurídico – ConJur, 26 jul. 2002. Disponível em: https://www.conjur.com.br/2002-jul-26/crimes_informatica/. Acesso em: **04 de fevereiro de 2026.**

ALEXANDRE JÚNIOR, J. C. Cibercrime: um estudo acerca do conceito de crimes informáticos. *Revista Eletrônica da Faculdade de Direito de Franca*, Franca, v. 14, n. 1, jun. 2019. Disponível em: https://www.revista.direitofranca.br/index.php/refdf/article/view/602/pdf. Acesso em: 05 fev. 2026.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

ROQUE, S. M. **Criminalidade informática:** crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007.

CAMARGO, Michel de Souza. *Crimes cibernéticos: desafios para a responsabilização dos autores de crimes virtuais.* 2020. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade Cristo Rei, Cornélio Procópio, 2020. Disponível em: https://repositorio.faccrei.edu.br/wp-content/uploads/2020/01/TCC-MICHEL-CAMARGO.pdf. Acesso em: 26 fev. 2026.

ROSA, Fabrízio. Crimes de Informática. 2.ed. Campinas: BookSeller, 2006.

GUIMARÃES, Pedro Vinícius. **Criminalidade virtual: desafios do direito brasileiro face ao avanço dos crimes cibernéticos**. 2024. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, Goiânia, 2024. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/7549/1/PEDRO%20VIN%C3%8DCIUS%20GUIMAR%C3%83ES.pdf. Acesso em: 14 mar. 2026.

JUSBRASIL. *A Lei Carolina Dieckmann: proteção à privacidade e combate aos crimes cibernéticos no Brasil*. JusBrasil, 14 dez. 2024. Disponível em: https://www.jusbrasil.com.br/artigos/a-lei-carolina-dieckmann-protecao-a-privacidade-e-combate-aos-crimes-ciberneticos-no-brasil/2919292428. Acesso em: 14 jan. 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: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 12 mar. 2026.

LIMA, Juliana Kelly Costa de; TROVÃO, Lidiana Costa de Sousa. A Lei n. 12.737/2012 – Carolina Dieckmann e seu impacto na sociedade para proteção de dados informáticos. *Revista Científica de Alto Impacto*, v. 27, Edição 127/OUT 2023, 18 out. 2023. Disponível em: https://revistaft.com.br/a-lei-n-12-737-2012-carolina-dieckmann-e-seu-impacto-na-sociedade-para-protecao-de-dados-informaticos/. Acesso em: 23 set. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 mar. 2026.

FRANÇA, Beatricia dos Santos Carvalho Pereira. Crimes cibernéticos e a legislação brasileira. *RevistaFT*, Ciências Sociais Aplicadas, v. 28, ed. 138, 2024. Disponível em: https://revistaft.com.br/crimes-ciberneticos-e-a-legislacao-brasileira/. Acesso em: 14 mar. 2026.

DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. *Revista de Direito*, v. 12, n. 22, p. 97-118, 2019.

ARAÚJO, Iran Carlos da Silva. **Os crimes cibernéticos e o direito penal brasileiro: proteção para quem?** JusBrasil, 2023. Disponível em: https://www.jusbrasil.com.br/artigos/os-crimes-ciberneticos-e-o-direito-penal-brasileiro/1894019562. Acesso em: 14 mar. 2026.

QUEIROZ, Gabriel Ferreira. **Cibercriminalidade no Brasil: aplicação, falibilidade e impunidade**. 2021. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/2960/1/TCC-%20GABRIEL%20FERREIRA%20QUEIROZ%20%20.pdf. Acesso em: 14 mar. 2026

DORIGON, Alessandro; SOARES, Renan Vinicius Oliveira**. Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 23, n. 5342, 15 fev. 2018. Disponível em: https://jus.com.br/artigos/63549. Acesso em: 04 fev. 2026.

SOUZA, A. P.; LIMA, C. F. **A investigação de crimes cibernéticos no Brasil: desafios operacionais e estruturais**. Revista Brasileira de Segurança Pública, v. 16, n. 3, p. 105-125, 2022. Disponível em: https://rbsp.org.br/edicoes/vol16num3/souza lima-investigacao-crimes-ciberneticos. Acesso em: 12 mar. 2026.

LOPES, M. C. **A complexidade da investigação criminal no ambiente digital: anonimato, criptografia e jurisdição transnacional**. Revista de Ciências Policiais, v. 14, n. 2, p. 55-78, 2021. Disponível em: https://revistacienciaspoliciais.org.br/edicoes/vol14num2/lopes-investigacao-criminal ambiente-digital. Acesso em: 12 mar. 2026.

FERREIRA, Mariana Figueiredo Gonçalves. **ESTELIONATO EM AMBIENTE VIRTUAL: Desafios para agências policiais em Minas Gerais a partir do olhar da complexidade e das Ciências Policiais**. 2024. Tese de Doutorado. Universidade do Estado de Minas Gerais. Disponível em: https://mestrados.uemg.br/images/ppgspcid/Disserta%C3%A7%C3%B5es/TURMA_- 4/FINAL __Mariana_Figueiredo.pdf. Acesso em: 03 mar. 2025.

FERREIRA, P. J. **A Convenção de Budapeste e o combate internacional ao crime cibernético: reflexões sobre os desafios da cooperação jurídica**. Revista Brasileira de Direito Internacional, v. 17, n. 1, p. 85-100, 2020. Disponível em: https://revistas.ufpr.br/rbdi/article/view/81344. Acesso em: 25 mar. 2025.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law (EJJL)*, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 06 mar. 2026.

BRASIL. Ministério da Fazenda. **1968 A 1981 – Começa a Era da Secretaria da Receita Federal**. Disponível em: < http://idg.receita.fazenda.gov.br/sobre/institucional/memoria/imposto-de-renda/historia/1968- a-1981-comeca-a-era-da-secretaria-da-receita-federal > Acesso em: 12 mar. 2026.

SOUZA, Luíza Ribeiro de Menezes. **Proteção de dados pessoais: estudo comparado do Regulamento 2016/679 do Parlamento Europeu e Conselho e o Projeto de Lei brasileiro n. 5.276/2016**. *Caderno Virtual*, Brasília, v. 1, n. 41, 2018. Disponível em: https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3153. Acesso em: 12 mar. 2026.

DONEDA, Danilo. **Da Privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 1

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf. Acesso em: 06 fev. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 mar. 2026.

MICROSOFT. **O que é um ataque cibernético**?. Microsoft, 2023. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-a-cyberattack. Acesso em: 11 mar. 2026.

MARQUES, Inácio de Melo. **Crimes digitais: roubo de dados e a responsabilidade jurídica**. *RevistaFT – Revista Científica Eletrônica Multidisciplinar*, v. 27, n. 129, dez. 2023. DOI: 10.5281/zenodo.10291882. Disponível em: https://revistaft.com.br/crimes-digitais-roubo-de-dados-e-a-responsabilidade-juridica/. Acesso em: 11 mar. 2026.

FAGUNDES, Jorge Alexandre. *As consequências do roubo de dados pessoais: uma análise dos impactos*. Jusbrasil, 15 maio 2023. Disponível em: https://www.jusbrasil.com.br/artigos/as-consequencias-do-roubo-de-dados-pessoais-uma-analise-dos-impactos/1835707405. Acesso em: 14 mar. 2026.

RODRIGUES, Samara. *Violação de dados: o que é, impactos e como evitar*. Educa Mais Brasil, 2024. Disponível em: https://www.educamaisbrasil.com.br/educacao/dicas/violacao-de-dados-o-que-e-impactos-e-como-evitar. Acesso em: 14 mar. 2026.