CRIMES CIBERNETICOS E SEUS IMPACTOS NOS PROCESSOS JUDICIAIS BRASILEIRO

CYBERCRIMES AND THEIR IMPACTS ON BRAZILIAN JUDICIAL PROCESSES

Thais Maria Ferreira da Silva[1]
Ernandes Pereira Rodrigues[2]

RESUMO: Os avanços tecnológicos moldam o comportamento humano e trazem conveniência e simplicidade. A *internet* tem inúmeros benefícios, mas também apresenta riscos de segurança digital. Sob tal ótica, este estudo tem como objetivo analisar como ocorre a prática dos crimes cibernéticos e quais as dificuldades para o combate desses delitos A metodologia empregada foi uma revisão de dados, informações e literaturas, analisando obras e publicações que abordaram o tema ao longo dos últimos anos, bem como pesquisas de publicações de artigos sobre o tema. Destarte, os resultados desta pesquisa mostram que apesar das evoluções que ocorreram no código penal brasileiro e criação das leis destinadas aos crimes cibernéticos, ainda não são suficientes para reduzir, penalizar e trazer segmentos necessários para que essa conduta possa ser diminuída. Com isso, são necessárias mais evoluções e ações do direito penal na busca de criminalizar essas práticas, conscientizar a população e ofertar segurança nesses meios virtuais. Este estudo contribui para discussões sobre reformas legislativas e diretrizes eficazes na prevenção dos crimes cibernéticos, reconhecendo a necessidade de equilíbrio entre direitos individuais e segurança cibernética. As considerações finais apontam que, embora o Brasil tenha avançado na criação de leis para combater crimes cibernéticos, essas medidas ainda são insuficientes para enfrentar a complexidade desses delitos, e que é crucial continuar aprimorando o direito penal, além de promover a conscientização pública sobre segurança digital. Somente com uma abordagem integrada será possível criar um ambiente virtual mais seguro e equilibrado entre direitos individuais e proteção coletiva.

Palavras-chave: Crimes cibernéticos; Processos; Judiciário; Impactos.

ABSTRACT: Technological advances shape human behavior and bring convenience and simplicity. The Internet has countless benefits, but it also presents digital security risks. From this perspective, this study aims to analyze how cybercrimes occur and what the difficulties are in combating these crimes. The methodology used was a review of data, information, and literature, analyzing works and publications that addressed the topic over the last few years, as well as research on published articles on the topic. Thus, the results of this research show that despite the developments that have occurred in the Brazilian penal code and the creation of laws aimed at cybercrimes, they are still not enough to reduce, penalize, and bring in the necessary segments so that this behavior can be reduced. Therefore, further developments and actions are needed in criminal law to seek to criminalize these practices, raise awareness among the population, and offer security in these virtual environments. This study contributes to discussions on legislative reforms and effective guidelines for preventing cybercrimes, recognizing the need for a balance between individual rights and cybersecurity. The final considerations indicate that, although Brazil has made progress in creating laws to combat cybercrimes, these measures are still insufficient to address the complexity of these crimes, and

[1] Aluna concludente do Curso de Bacharelado em Direito, da Faculdade do Cerrado Piauiense-FCP. E-mail: mariathais192001@gmail.com

[2] Orientador de conteúdo deste artigo, formado em Bacharelado em Direito, com especialização em gestão pública municipal. E-mail: drernandes@hotmail.com

that it is crucial to continue improving criminal law, in addition to promoting public awareness about digital security. Only with an integrated approach will it be possible to create a safer virtual environment that balances individual rights and collective protection.

Keywords: Cybercrimes; Law Suit; Judiciary; Impacts.

INTRODUÇÃO

Os avanços tecnológicos proporcionaram inúmeros benefícios à sociedade, mas também introduziram novos desafios no campo dos crimes cibernéticos. No Brasil, a crescente incidência desses crimes demonstra uma lacuna tanto na legislação quanto nos mecanismos de combate e nas estruturas investigatórias. Esse cenário reflete não só a rápida evolução das tecnologias digitais, mas também a adaptação dos criminosos a esses novos ambientes virtuais, explorando vulnerabilidades e utilizando métodos cada vez mais sofisticados para fraudes, roubo de dados, ataques de *ransomware* e outras atividades ilícitas.

A hipótese deste estudo sugere que a ineficácia na punição dos crimes virtuais decorre da falta de atualização dos processos investigativos e da carência de profissionais especializados na área de perícia digital, o que compromete a responsabilização dos criminosos e, consequentemente, o andamento justo dos processos judiciais. Além disso, a ausência de um marco regulatório suficientemente robusto e adaptado às novas modalidades de crimes digitais dificulta o estabelecimento de padrões claros para a coleta e preservação de provas eletrônicas, bem como para a colaboração entre instituições nacionais e internacionais.

Essa deficiência na regulamentação, aliada à falta de infraestrutura tecnológica e de recursos destinados ao combate a esses crimes, resulta em investigações inconclusivas, provas comprometidas e processos lentos, gerando insegurança jurídica e, muitas vezes, impunidade. Assim, esta pesquisa visa explorar não apenas as dificuldades técnicas e institucionais que impactam a eficácia das ações judiciais, mas também propor soluções para fortalecer o sistema investigativo, a capacitação de profissionais especializados e o desenvolvimento de políticas públicas que acompanhem o avanço das ameaças cibernéticas.

Os desafios criados com a chegada dos crimes cibernéticos redirecionam aos seguintes problemas do presente artigo: Haverá a devida capacidade por parte das estruturas jurídicas e tecnológicas brasileiras de enfrentar a complexidade dos crimes cibernéticos? Como os crimes cibernéticos impactam a sociedade brasileira?

A justificativa para este estudo reside no fato de que crimes cibernéticos representam uma crescente ameaça à segurança tanto de indivíduos quanto de instituições. O aumento da

criminalidade digital exige uma modernização dos sistemas de combate, que atualmente se mostram ineficazes devido à falta de uma infraestrutura adequada e de especialistas capacitados para realizar perícias digitais complexas, afetando diretamente a capacidade de responsabilização e punição dos criminosos.

Objetiva-se de modo específico: Analisar os tipos mais comuns de crimes cibernéticos e as facilidades envolvidas na sua execução; examinar os desafios técnicos e legais enfrentados pelas autoridades na investigação desses crimes no Brasil; e propor soluções para melhorar as políticas públicas e a capacitação profissional, visando o combate mais eficiente à criminalidade digital.

A pesquisa sobre crimes cibernéticos no Brasil e seus impactos nos processos judiciais abrange quatro eixos centrais que visam compreender, legislar, avaliar e propor soluções para esse fenômeno crescente. O primeiro eixo, Crimes Cibernéticos, investiga delitos como invasão de dispositivos, fraudes e *cyberstalking*. Abrange os Desafios no Processo Investigatório e Medidas de Prevenção. A pesquisa também explora a Legislação Brasileira e Convenção de Budapeste, abordando a adequação do Brasil aos padrões internacionais. Além disso, as Leis Penais e Crimes Cibernéticos incluem a Lei Carolina Dieckmann, que criminaliza invasões digitais e se destaca como referência nacional.

1 DOS CRIMES CIBERNETICOS

Atualmente, o avanço tecnológico contínuo trouxe novos desafios legais ligados aos chamados crimes cibernéticos. Embora o Código Penal brasileiro não ofereça uma definição exata para esses crimes, é possível entendê-los com base na legislação vigente e na complexidade das ações criminosas realizadas no ambiente digital.

1.1 CONCEITO DO CRIME CIBERNÉTICO E CRIMES MAIS FREQUENTES

A complexidade e a dinâmica desse campo específico da criminalidade digital tornam desafiadora a criação de uma nomenclatura única e estabelecida. Diversos termos são utilizados para descrever atividades ilícitas que envolvem o uso de dispositivos eletrônicos, manipulação de redes de dados e ofensas a bens jurídicos, entre outros aspectos relevantes. Nesse contexto, é essencial entender as diferentes perspectivas e abordagens adotadas pelos estudiosos sobre o tema.

Assim, não há um consenso doutrinário consolidado sobre o conceito de crime cibernético, sendo que a principal diferença reside na terminologia utilizada. A definição de crimes cibernéticos pode ser resumida como atividades ilegais praticadas com o uso de dispositivos eletrônicos, conectados ou não à *internet*. Esses crimes também incluem ataques a equipamentos tecnológicos, sistemas de informação e bancos de dados.

Essas ações criminosas exploram as vulnerabilidades do mundo digital, abrangendo desde fraudes e invasões até a disseminação de códigos maliciosos. O núcleo dos crimes cibernéticos está na violação das normas que regulam o uso ético e legal da tecnologia, o que representa um constante desafio para a legislação penal moderna. O Código Penal não define o que é crime cibernético, porém o artigo 1° da Lei de Introdução ao Código Penal traz em seu *caput* a seguinte definição de crime:

> Art 1º Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas.

O conceito de crimes cibernéticos não é uniforme. Para Teixeira (2023, p. 1160):

> Crime de informática é aquele que, quando praticado, utiliza–se de meios informáticos como instrumento de alcance ao resultado pretendido, e também aquele praticado contra os sistemas e meios informáticos. Por meios informáticos devemos compreender os hardwares e softwares de computadores, tablets, smartphones, entre outros dispositivos que possam ser utilizados para a prática delitiva.

Os crimes virtuais, também conhecidos como crimes de informática, podem ser descritos como ações humanas que, dentro do direito penal, são caracterizadas como atos típicos, ilícitos e culpáveis. Nesses crimes, um dispositivo digital é utilizado para facilitar ou consumar a atividade criminosa, causando prejuízos a terceiros, independentemente de trazer ou não benefícios ao autor do crime.

Entre os crimes virtuais mais comuns estão a pirataria, a pornografia infantil, os crimes contra a honra e a espionagem. Assim, os cibercrimes podem ser definidos como delitos praticados no ambiente digital ou relacionados a informações digitais, por meio de diversos dispositivos conectados à *internet*, como computadores, celulares, *smartphones* e *tablets*, entre outros (Nascimento, 2019).

Em síntese, ainda que o Código Penal brasileiro não defina especificamente o que constitui um crime cibernético, a Lei de Introdução ao Código Penal estabelece diretrizes gerais para identificar uma infração penal. Exemplos como pirataria, pornografia infantil, crimes contra a honra e espionagem demonstram a variedade de crimes possíveis no meio digital. Dessa

forma, é essencial que o sistema jurídico e as autoridades estejam preparados para enfrentar essa complexa expansão dos crimes cibernéticos e proteger a sociedade de seus efeitos.

1.2 DESAFIOS NO PROCESSO INVESTIGATÓRIO E MEDIDAS DE PREVENÇÃO

Quando se fala em crimes cibernéticos, um grande desafio surge na coleta e na organização de provas, já que a principal dificuldade nas investigações desses delitos é a escassez de evidências que comprovem a atividade criminosa em questão. Portanto, é crucial enfatizar a importância e a complexidade das investigações para a responsabilização dos criminosos.

Entre os vários métodos de obtenção de provas, a perícia se destaca de maneira significativa na investigação de crimes virtuais, pois pode estabelecer de forma definitiva tanto a ocorrência do ato criminoso quanto a identificação do autor. Essa perícia é realizada por um especialista, conhecido como perito, que possui o conhecimento técnico necessário para examinar, por exemplo, um dispositivo que foi identificado por meio da análise de vestígios coletados e apreendidos. Através desse processo, novos vestígios relacionados ao crime podem ser reunidos como provas materiais no processo, contribuindo assim para a formação da convicção das autoridades competentes.

A primeira etapa da investigação consiste na identificação do meio utilizado para a prática do crime, como *e-mail*, *websites* ou salas de bate-papo, já que cada um desses meios exige um caminho investigativo distinto. Outro aspecto a ser destacado é que o investigador deve garantir a proteção do computador utilizado para a coleta de dados, adotando todas as precauções necessárias para evitar ataques digitais que possam comprometer ou destruir informações ou até mesmo permitir o acesso remoto a um terceiro.

O combate à criminalidade cibernética enfrenta diversos obstáculos, não apenas em relação às lacunas na legislação, mas também devido às implicações que podem surgir em termos de restrição à liberdade de expressão e ao rápido avanço da tecnologia. A falta de fronteiras claras na jurisdição pode levar a questões sobre soberania nacional, especialmente quando vários países estão envolvidos.

Essa indefinição de fronteiras dificulta a determinação do local onde os dados estão armazenados e qual país deve ser responsabilizado pelos danos causados, bem como a identificação dos locais onde o crime ocorreu e produziu efeitos, e a definição de elementos como autoria e culpabilidade, o que torna os procedimentos de investigação ainda mais complexos (Teixeira, 2023).

No que diz respeito ao local do crime e à jurisdição para julgá-lo, o Código Penal brasileiro adota o princípio da territorialidade como regra geral, o que significa que a legislação do Estado se aplica a eventos ocorridos dentro do território nacional, conforme disposto no artigo 5º.

Além disso, considera-se que o crime foi cometido no local onde a ação ou omissão ocorreu, total ou parcialmente, assim como onde ocorreu ou deveria ter ocorrido o resultado, conforme estabelecido no artigo 6º do Código Penal. No entanto, o artigo 7º do Código Penal apresenta algumas exceções em que a lei brasileira pode ser aplicada a crimes cometidos no exterior ou perpetrados a partir de fora do país.

1.3 MEDIDAS DE PREVENÇÃO E COMBATE AOS CRIMES CIBERNÉTICOS

Dentre as medidas que o Governo Federal se dispôs a fazer foi, por meio do Ministério da Justiça e Segurança Pública (MJSP), o lançamento em 22 de março de 2023, do primeiro Plano Tático de Combate a Crimes Cibernéticos, com o objetivo de prevenir e reprimir esse tipo de crime no país.

Um dos pontos do Plano Tático é um Acordo de Cooperação entre a Polícia Federal e a Federação Brasileira de Bancos (Febraban) que facilitará o compartilhamento de informações, visando medidas preventivas e educativas, de forma a tornar o espaço cibernético mais seguro, identificando e punindo organizações criminosas.

A Federação Brasileira de Bancos (Febraban) é uma das entidades privadas que auxiliaram e incentivaram a construção do Plano Tático de Combate a Crimes Cibernéticos. O Plano Tático prevê a criação de um banco de dados de ocorrências, que terá o amplo acesso das polícias judiciárias da União e dos estados. Dessa forma, os modelos de investigações e soluções de crimes poderão ser replicados de forma eficiente em todo o país.

Será criado, ainda, um programa de prevenção a fraudes bancárias eletrônicas, golpes digitais e a capacitação de agentes de segurança para que possam lidar com os vários tipos de crime que cada vez mais são corriqueiros no dia a dia do brasileiro. No mais, será montada uma estrutura integrada com a participação de forças de segurança federais e estaduais, entidades públicas e privadas nacionais e internacionais e especialistas na temática. Juntos, eles vão se especializar para atuar no enfrentamento às organizações criminosas que atuam em crimes digitais.

O Plano Tático de Combate a Crimes Cibernéticos contém eixos temáticos que destacam a prevenção e a mitigação de ameaças cibernéticas; o gerenciamento de riscos e incidentes

decorrentes da criminalidade cibernética; o aprimoramento de infraestruturas críticas para combate a crimes cibernéticos; o amparo legal e regulamentar; as parcerias nacionais e cooperação internacional; a padronização e a integração informacional; além de pesquisa, desenvolvimento, inovação e educação para o enfrentamento a crimes cibernéticos.

1.4 LEGISLAÇÕES BRASILEIRA E A CONVENÇÃO DE BUDAPESTE

É indispensável que o legislador exerça um papel fundamental ao elaborar leis que tratem de forma específica os eventos ocorridos no ambiente digital. Esse esforço é necessário para assegurar a proteção das garantias fundamentais previstas na Constituição, como:

> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, trouxe uma importante atualização ao Código Penal Brasileiro no que se refere aos crimes cibernéticos e delitos virtuais. O nome da lei faz referência a um caso amplamente divulgado, em que a atriz Carolina Dieckmann teve seu computador invadido por um *hacker* que divulgou suas fotos íntimas.

Essa legislação incluiu os artigos 154-A e 154-B no Código Penal e alterou os artigos 266 e 298. Seu conteúdo abrange crimes relacionados ao uso indevido de informações e materiais pessoais que afetam a privacidade de indivíduos na *internet*, como imagens e vídeos.

Mais tarde, foi promulgada a Lei nº 12.965/2014, conhecida como Marco Civil da Internet:

> A Lei nº 12.965/2014, em vigor desde 23 de junho de 2014, trouxe várias disposições que, apesar de terem um caráter 'civil', também influenciam na investigação de crimes virtuais. Essa lei trata da preservação de dados de provedores de acesso à internet, que são obrigados a armazenar registros de conexão de usuários, como data, hora, duração e endereço IP, por um ano, mantendo-os em sigilo. (Othon; Damasceno, 2023, p.13).

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, representa um marco recente na legislação para assegurar a proteção dos direitos fundamentais de liberdade, privacidade e desenvolvimento pessoal. Essa lei define normas para o tratamento de dados pessoais dos cidadãos, abrangendo tanto o meio físico quanto o digital. Com o aumento do uso de dados de usuários para aprimorar experiências digitais, a Lei Geral de Proteção de Dados (LGPD) tem papel crucial ao regulamentar essas práticas e assegurar instrumentos legais que protejam a privacidade de cada indivíduo (Pinheiro, 2022).

Em 31 de março de 2021, entrou em vigor a Lei nº 14.132/21, conhecida como Lei de *Stalking*, que adicionou o artigo 147-A ao Código Penal, tornando a perseguição um crime. Essa lei visa proteger a liberdade individual contra comportamentos que invadem profundamente a privacidade de alguém e limitam o exercício de suas liberdades básicas.

A Lei de *Stalking* preenche uma lacuna na legislação, estabelecendo punições proporcionais para condutas de perseguição, que antes eram tratadas como contravenções com penas leves. Com essa nova legislação, a perseguição passou a ser punida com pena de reclusão de seis meses a dois anos (Cunha, 2021).

Além disso, o Governo Federal ratificou a Convenção sobre o Crime Cibernético de Budapeste, reforçando a cooperação internacional no combate aos crimes cibernéticos. A adesão a essa convenção multilateral proporciona ao Brasil recursos adicionais para investigar crimes cibernéticos e infrações que envolvem evidências digitais em outros países.

O Decreto nº 11.491, formalizando essa adesão, foi publicado no Diário Oficial da União em 12 de abril de 2023, visando fortalecer a cooperação rápida e eficiente com parceiros estratégicos. Sofia Jacob explica que a Convenção estabelece uma série de medidas para os países signatários com o objetivo de prevenir, investigar e punir crimes cibernéticos.

A Convenção de Budapeste inclui a definição de delitos relacionados à tecnologia da informação, a promoção de colaboração internacional em investigações e a criação de legislações específicas para reprimir essas atividades criminosas. Os países signatários da convenção se comprometem a adotar ações eficazes para evitar crimes cibernéticos e a fomentar a cooperação global no combate a esses delitos. A convenção também prevê a criação de unidades especializadas em investigação, o compartilhamento de informações entre autoridades responsáveis e a cooperação internacional para viabilizar a extradição de suspeitos envolvidos em crimes cibernéticos.

2 LEI GERAL DE PROTEÇÃO DE DADOS E A BUSCA POR SEGURANÇA DIGITAL

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) foi criada em resposta ao aumento das preocupações com a privacidade e segurança dos dados pessoais no meio digital. A lei reforça a importância de proteger esses dados, dando aos titulares maior controle sobre suas informações.

Em relação ao conceito de dados pessoais, o artigo 5º, inciso I, da Lei Geral de Proteção de Dados (LGPD) define o termo como “informação relacionada a pessoa natural identificada

ou identificável". Em outras palavras, dado pessoal é qualquer informação que possibilite identificar uma pessoa, seja de forma direta ou indireta.

A proteção aos dados pessoais visa, portanto, não apenas resguardar os indivíduos (sejam pessoas físicas ou jurídicas) contra o uso inadequado de suas informações, mas também aumentar a segurança, dificultando que criminosos cibernéticos acessem dados sensíveis por meio de vulnerabilidades.

Para casos de descumprimento da lei, a Lei Geral de Proteção de Dados (LGPD) estabelece sanções rigorosas, como advertências, multas significativas e até a possibilidade de impedir o tratamento de dados. No artigo 52, a lei lista essas penalidades administrativas, que servem como um forte incentivo para que empresas adotem práticas rigorosas de segurança digital.

Assim, a Lei Geral de Proteção de Dados (LGPD) contribui para prevenir vazamentos de dados ao impor requisitos rígidos de segurança. As empresas devem adotar avançadas medidas de cibersegurança para evitar acessos não autorizados e proteger dados sensíveis de ataques digitais

Apesar dessas medidas, ainda há casos de vazamento de dados. No Brasil, o caso Cyrela foi o primeiro em que uma empresa foi condenada com base na Lei Geral de Proteção de Dados (LGPD), como descrito por Lima (2022).

> A Cyrela é uma das maiores empresas brasileiras do ramo imobiliário, com operações em outros 16 estados, além de São Paulo, e também no exterior. Fabrício Coelho foi o réu que moveu a ação por danos morais contra a construtora, por ter seus dados fornecidos a empresas de arquitetura, instituições financeiras e outras companhias, após a compra de um apartamento. A decisão foi emitida no dia 29 de setembro de 2020 pela juíza Tonia Yuka Koroku, que julgou em favor do réu, decidindo que a Cyrela violou os princípios da proteção e da finalidade específica previstos na LGPD. Isso porque o contrato estipula a possibilidade de inclusão dos dados do cliente no banco de dados, mas não especifica sua finalidade. Segundo a magistrada, a prática também desrespeitou o Código de Defesa do Consumidor, que garante o direito à 'informação adequada e clara' sobre serviços e à proteção contra 'métodos comerciais coercitivos ou desleais'. Em sua decisão, ela destacou ainda que a Constituição estabelece 'a honra, o nome, a imagem, a privacidade, a intimidade e a liberdade' como direitos fundamentais.

O caso ilustra as consequências legais e éticas dos vazamentos de dados, destacando a necessidade urgente de que empresas adotem medidas eficazes de segurança e transparência. Esse episódio reforça a importância de uma gestão cuidadosa dos dados pessoais, não apenas para evitar complicações legais, mas também para manter a confiança dos consumidores e preservar a reputação da empresa no mercado.

Apesar da frequência com que a Lei Geral de Proteção de Dados (LGPD) é invocada em ações judiciais, nem sempre resultam em penalidades indenizatórias. Um levantamento de 2021 revelou que, entre 465 decisões envolvendo a Lei Geral de Proteção de Dados (LGPD), 77% não resultaram em condenação (Paiva, 2022).

Esse panorama pode refletir diferentes interpretações nos tribunais, desafios na aplicação da lei ou a necessidade de ajustes nas estratégias de ação. Vale lembrar que a Lei Geral de Proteção de Dados (LGPD) é uma legislação recente. O alto índice de decisões sem condenação sugere que empresas e organizações ainda estão se ajustando às novas exigências. É possível que, à medida que as práticas de proteção de dados amadureçam, as decisões judiciais também evoluam.

Para compreender melhor a aplicação e interpretação da Lei Geral de Proteção de Dados (LGPD), é importante considerar a complexidade do cenário jurídico. À medida que mais casos forem julgados, o desenvolvimento de uma jurisprudência sólida será fundamental para estabelecer diretrizes consistentes no tratamento das questões de proteção de dados no Brasil.

3 LEI Nº 14.132/2021 E O *CYBERSTALKING*

É perceptível que a legislação brasileira tem se adaptado conforme surgem novas formas de interação proporcionadas pela tecnologia. Nas últimas décadas, as redes sociais se tornaram extremamente populares, encurtando distâncias e facilitando a comunicação entre pessoas. Hoje, é possível interagir facilmente com indivíduos de praticamente qualquer lugar e acompanhar aspectos da vida de outras pessoas.

Nesse contexto, destaca-se a Lei nº 14.132/2021, que tipificou uma das condutas criminosas mais relevantes no ambiente digital: o *cyberstalking*. O termo "*stalking*", derivado do verbo inglês "*to stalk*", significa perseguir, vigiar ou espionar.

Essa prática pode ocorrer por várias razões, sendo uma das mais comuns o término de um relacionamento amoroso, em que uma das partes, não aceitando o fim, invade a privacidade e a integridade psicológica da outra pessoa de forma repetitiva e insistente. Esse comportamento pode escalar, gerando riscos à integridade física e até à vida da vítima. Conforme observa a psicóloga e criminóloga italiana Micoli (2012, p. 12):

> [...] o *stalking* é uma forma de agressão psicológica e física direta, que visa sobrepujar a vontade da vítima, destruir sua moral e sua capacidade de resistência por meio de um gotejamento incessante, em um contexto de crescente perseguição, insistente como os pingos que, com o passar do tempo, escavam a pedra. O *stalker* persegue,

> ameaça, maltrata a vítima, fazendo com que nasça nesta um estado de ansiedade e medo que pode chegar a comprometer o desenvolvimento normal do seu cotidiano. (grifos da autora).

Assim, evidencia-se a complexidade e a gravidade do fenômeno do *stalking*, que vai além da simples ideia de perseguição. A descrição do comportamento do agressor como um "gotejamento incessante" é uma metáfora que ilustra de forma vívida a persistência e a natureza insidiosa desse tipo de violência. O efeito não se restringe ao psicológico da vítima, pois há uma intenção clara de enfraquecer sua resistência e afetar sua moral.

A comparação com "pingos que escavam a pedra" sugere um processo gradual, mas implacável, indicando que, com o tempo, o *stalking* pode corroer a integridade emocional da vítima. Essa abordagem que considera tanto os impactos físicos quanto psicológicos ressalta a importância de compreender o *stalking* de forma mais ampla, como uma estratégia de agressão multifacetada.

A partir disso, surge o conceito de *cyberstalking*, adaptando esse comportamento ao ambiente virtual. No *cyberstalking*, o agressor utiliza meios digitais para perturbar a vítima de maneira invasiva e indesejada. Como aponta Brito (2013, p. 84):

> [...] a exemplo do que ocorreu com o *bullying*, o *stalking* ganhou uma ferramenta que facilitou o serviço do perseguidor (*stalker*), e potencializou os danos causados às vítimas. Emails, tweets, visitas de perfil e até as famosas 'cutucadas' podem servir de exemplos de novos meios de execução proporcionados pelo uso da internet, passando com isso a denominar-se *Cyberstalking*.

Assim, para que o *stalking* virtual seja caracterizado, é essencial que a conduta ocorra através de meios digitais, como redes sociais, *e-mails*, entre outros. Nesse sentido, Crespo (2015) também reforça essa ideia:

> O *cyberstalking* é, portanto, o uso da tecnologia para perseguir alguém e se diferencia da perseguição '*offline*' (ou mero *stalking*) justamente no que tange o modus operandi, que engloba o uso de equipamentos tecnológicos e o ambiente digital. Além disso, o *stalking* e o *cyberstalking* podem se mesclar, havendo as duas formas concomitantemente. O *stalker* – indivíduo que pratica a perseguição – mostra-se onipresente na vida da sua vítima, dando demonstrações de que exerce controle sobre ela, muitas vezes não se limitando a persegui-la, mas também proferindo ameaças e buscando ofendê-la ou humilhá-la perante outras pessoas. Curiosamente o *cyberstalking* é cometido, muitas vezes, não por absolutos desconhecidos, mas por pessoas conhecidas, não raro por ex-parceiros como namorados, ex-cônjuge, etc.

Outro elemento fundamental para caracterizar o *cyberstalking* é a invasão da privacidade da vítima sem seu consentimento, ou seja, a perseguição ocorre de maneira indesejada e contra a vontade da vítima. Nesse contexto, em 2021, a Lei nº 14.132 foi introduzida para alterar o

Código Penal brasileiro, tipificando a conduta de *stalking*, incluindo o *cyberstalking*, com a seguinte redação:

> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.

Ao analisar o que a legislação dispõe, alguns aspectos relevantes corroboram o conceito de *stalking* e *cyberstalking*. Com o termo "reiteradamente," o legislador ressalta que a prática do *stalking*, incluindo o *cyberstalking*, exige repetição da ação, ou seja, uma conduta isolada não configura o crime; é necessário que o comportamento do agente seja habitual.

Outro ponto importante é a abrangência da tipificação, que alcança o ambiente digital. A expressão "por qualquer meio" amplia o crime de perseguição, englobando também o meio virtual, e, assim, contempla o *cyberstalking*. A Lei nº 14.132/2021 representa um avanço importante, reconhecendo o caráter multifacetado do *stalking*, inclusive no âmbito digital. Criar mecanismos que acompanhem a rápida evolução das formas de perseguição é essencial para que a legislação proteja efetivamente as vítimas, independentemente do meio utilizado pelos perseguidores.

Essa necessidade de uma abordagem diferenciada na criação de leis para a tecnologia da informação evidencia a complexidade do tema e a importância de uma legislação que se adapte ao contexto atual. A expressão "ordenação jurídica natimorta" alerta para o risco de leis que, ao não acompanharem o ritmo das mudanças tecnológicas, se tornam obsoletas desde sua concepção.

É necessário, portanto, que o legislador atue com cautela para evitar a criação de normas que se tornem rapidamente desatualizadas e insuficientes diante dos avanços contínuos da tecnologia. Essa visão ressalta a importância de uma abordagem proativa na elaboração de normas para a tecnologia da informação, prevendo desenvolvimentos futuros e garantindo que as leis continuem pertinentes. Esse tipo de reflexão é fundamental para assegurar que as normas jurídicas sejam eficazes e duradouras em um ambiente tão dinâmico e inovador como o da tecnologia da informação.

4 LEIS PENAIS E CRIMES CIBERNÉTICOS: ANÁLISE NO CONTEXTO BRASILEIRO

A análise dos crimes de fraude digital no Brasil exige uma compreensão detalhada das leis penais brasileiras e de sua aplicação a delitos virtuais. Neste estudo, serão avaliadas leis

penais relevantes que abordam crimes cibernéticos, com destaque para sua estrutura e eficácia no combate a esses crimes.

No Brasil, o sistema legislativo segue o princípio da reserva legal, assegurado pela Constituição Federal e pelo Código Penal. Assim, observa-se que apenas a lei pode criar e definir crimes e contravenções, além de estabelecer as penas correspondentes. Nas palavras de Jesus e Milagre (2016, p. 13):

> Não há crime, sem lei anterior que o defina. Especialmente quando tratamos de tecnologia da informação, a técnica para criar leis deve ser outra. Isto porque o legislador deve ter o cuidado para que não conceba uma ordenação jurídica natimorta, que ingressa no arcabouço legislativo de modo ultrapassado.

É relevante, portanto, refletir sobre a relação entre a legislação e a evolução da tecnologia da informação. Ao afirmar que "não há crime sem lei anterior que o defina," Jesus e Milagre (2016) destacam a importância da precisão e clareza das normas legais, especialmente em um contexto tão dinâmico como o da tecnologia da informação.

A tipificação dos crimes cibernéticos no Brasil está baseada no Código Penal e em leis complementares. É fundamental examinar como essas normas tratam as condutas específicas relacionadas à fraude digital e de que forma os tipos penais estão definidos. Entre as principais leis e regulamentações, o Código Penal se destaca por contemplar crimes relacionados ao ciberespaço, como estelionato, furto com fraude e crimes contra a honra, incluindo difamação. A Lei nº 12.737/2012 (conhecida como Lei Carolina Dieckmann) introduziu punições específicas para invasão de dispositivos e obtenção não autorizada de dados.

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) regulamenta o uso de dados pessoais e estabelece sanções administrativas para vazamentos de dados, uma questão diretamente ligada a crimes cibernéticos. Além disso, a Lei nº 14.132/2021 criou a tipificação para os crimes de *stalking* e *cyberstalking*, em uma iniciativa importante contra práticas criminosas que ocorrem tanto no ambiente físico quanto no virtual.

4.1 CÓDIGO PENAL BRASILEIRO E OS DESAFIOS DA ADAPTAÇÃO À ERA DIGITAL

O Código Penal Brasileiro, instituído em 1940, é um componente essencial do sistema jurídico do país. Contudo, ao lidar com os desafios apresentados pelos crimes cibernéticos, que emergem com o avanço da tecnologia e possibilitam novas práticas criminosas no ambiente virtual, é relevante discutir a necessidade de atualização na legislação, para que possa se alinhar melhor ao progresso tecnológico e às novas formas de delitos.

De acordo com o ministro do Superior Tribunal de Justiça, Cruz (2014), o Direito ainda não está completamente preparado para enfrentar os desafios impostos pelo desenvolvimento cibernético e pela criminalidade digital, conforme mencionado por Galli (2017, p. 105):

> A tecnologia de troca de dados proporcionada pela internet tem características que 'atraem' a prática de crimes, como o anonimato, dificuldades de rastreamento, abrangência potencialmente ilimitada de vítimas, eficiência e rapidez na troca de informações, inexistência de fronteiras e debilidade dos meios de tutela penal.

O ministro Cruz (2014) analisa de forma perspicaz as características específicas da tecnologia de troca de dados pela *internet*, ressaltando como esses aspectos podem fomentar a prática de crimes. O exame do ministro enfatiza diversos fatores que tornam o ambiente digital propício a atividades ilícitas.

A menção ao anonimato ilustra a facilidade com que os criminosos conseguem esconder suas identidades *online*, o que dificulta investigações e torna o rastreamento uma tarefa complicada. A potencialmente ilimitada abrangência de vítimas evidencia a escala global dos crimes cibernéticos, onde um único ataque pode afetar diversos indivíduos, organizações ou até países inteiros.

A rapidez e a eficiência da troca de informações na *internet* são apontadas como um atrativo para os criminosos, pois possibilitam a disseminação instantânea de dados maliciosos. A observação sobre a falta de fronteiras ressalta a natureza transnacional dos crimes cibernéticos, que muitas vezes transcendem as jurisdições tradicionais.

Além disso, a menção à fragilidade dos meios de proteção penal indica um desafio enfrentado pelas autoridades legais na defesa contra crimes *online*, destacando a necessidade de discutir a criação de instrumentos legais mais robustos e adaptados ao ambiente digital. A aplicação de tipos penais tradicionais, como estelionato e furto mediante fraude, exige interpretações flexíveis para abranger as particularidades dos crimes virtuais. A adaptação do Código Penal à dinâmica do mundo digital é essencial para garantir uma resposta jurídica eficaz e proporcional à natureza dessas práticas. A evolução contínua das técnicas virtuais demanda uma revisão constante, assegurando que a legislação esteja em sintonia com os novos desafios que surgem.

4.2 A LEI CAROLINA DIECKMANN: A FALTA DE EFICÁCIA E MODIFICAÇÕES

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, foi estabelecida em resposta a um caso de grande repercussão nacional que envolveu o vazamento de fotos íntimas

da atriz Carolina Dieckmann na *internet*. Sancionada em dezembro de 2012, a legislação visava principalmente criminalizar condutas associadas a crimes cibernéticos, especialmente a invasão de dispositivos eletrônicos e a obtenção não autorizada de dados.

Essa lei foi elaborada para preencher lacunas na legislação brasileira relacionada a delitos cometidos no ambiente digital. A criação de mecanismos legais que prevenissem e punissem práticas prejudiciais nesse contexto tornou-se essencial, pois, antes de sua promulgação, o sistema jurídico carecia de dispositivos específicos para enfrentar as crescentes ameaças cibernéticas. Com a promulgação da lei, foram acrescentados ao Código Penal brasileiro os artigos 154-A e 154-B, cuja redação original era:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa [...]
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos [...].

Ademais, os artigos 266 e 298 do mesmo código penal foram alterados pela referida lei, considerando as ações realizadas com esses dispositivos como crimes cibernéticos.

No entanto, como acontece com qualquer legislação, a Lei Carolina Dieckmann trouxe consigo desafios e fraquezas. Surgiram diversas críticas, principalmente em relação às penas estabelecidas, que foram consideradas leves diante do avanço tecnológico e do contexto atual. Em um ambiente virtual cada vez mais integrado à vida pessoal da sociedade, as condutas criminosas nesse espaço se tornam cada vez mais graves e causam danos significativos às vítimas.

A redação da lei também foi alvo de duras críticas, especialmente pelo fato de mencionar apenas a conduta criminosa "mediante violação indevida de mecanismo de segurança". Essa previsão foi considerada inadequada, uma vez que nem sempre os atos criminosos ocorrem por meio dessa violação.

Em 2021, foi promulgada a Lei nº 14.155/2021, que alterou a Lei Carolina Dieckmann, abordando os pontos mencionados, com penas mais severas para os infratores e eliminando o requisito de que a conduta fosse “mediante violação indevida de mecanismo de segurança”, entre outras modificações.

Entretanto, uma crítica importante que ainda persiste diz respeito ao núcleo do tipo penal. Observa-se que o verbo "invadir" não reflete adequadamente uma conduta relacionada à informática. O termo utilizado pelo legislador sugere uma ação que implica violência ou ameaça, o que é incomum em crimes no ambiente digital. Na maioria das vezes, o *hacker* utiliza alguma falha de segurança ou até mesmo a autorização da vítima para realizar sua conduta criminosa, conforme mencionado por Castro (2012).

Isso significa que, em casos de acesso remoto, não se pode afirmar que o agente malintencionado agiu de forma violenta para obter os dados do usuário. O que ocorre é a aplicação de artifícios. Para resumir a situação, muitas vezes é o próprio usuário que acaba permitindo que seus dados sejam acessados.

Portanto, embora se noticiem frequentemente invasões de servidores ou empresas por *hackers* que acessam indevidamente informações, é importante ter em mente que isso só ocorre porque o próprio usuário permitiu, mesmo que por falta de conhecimento sobre o funcionamento do sistema computacional, e por isso se tornou vítima de um engano.

Nesse contexto, o professor e advogado Castro (2012) apresenta uma análise crítica sobre o termo "invadir" no âmbito da Lei Carolina Dieckmann, destacando a ausência de violência física ou acesso remoto forçado por parte do agente mal-intencionado. Ele ressalta que, na maioria das situações, o que acontece é o uso de artifícios. Essa observação é crucial para entender a natureza das ações cibernéticas, nas quais o usuário frequentemente permite inadvertidamente o acesso a seus dados.

A ênfase na participação involuntária do usuário, que permite o acesso a suas informações por meio de truques, destaca a importância da conscientização e educação digital. A necessidade de medidas preventivas, como a promoção da cibersegurança e a conscientização sobre práticas seguras no uso de dispositivos digitais, é reforçada pelo fato de que a intrusão só ocorre devido ao desconhecimento do usuário sobre o funcionamento de um sistema computacional.

Essa visão destaca a complexidade das interações cibernéticas e a necessidade de abordagens legislativas que considerem não apenas as atividades criminosas, mas também a conscientização para reduzir vulnerabilidades e prevenir comportamentos prejudiciais no ambiente digital.

METODOLOGIA

Para esta pesquisa sobre crimes cibernéticos e seus impactos nos processos judiciais brasileiros, a abordagem utilizada foi qualitativa, com foco na análise documental e interpretação de textos legais e acadêmicos. O método de pesquisa adotado foi uma revisão bibliográfica crítica e sistemática, que envolveu a seleção e análise de fontes primárias, como legislações específicas e jurisprudências, e fontes secundárias, como artigos acadêmicos, livros e relatórios técnicos relevantes ao tema.

A escolha pela abordagem qualitativa se justifica pela complexidade do fenômeno dos crimes cibernéticos, que exige uma compreensão aprofundada dos marcos legais e suas implicações para o sistema jurídico. A análise das legislações, incluindo a Lei Geral de Proteção de Dados (LGPD), a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e a Lei nº 14.132/2021, permitiu investigar como essas normativas moldam o tratamento jurídico dos crimes digitais no Brasil e quais são os desafios enfrentados por magistrados e operadores do direito para lidar com essa nova realidade.

De acordo com Gil (2019), a pesquisa bibliográfica constitui uma etapa essencial em projetos de pesquisa, fornecendo a fundamentação teórica necessária para identificar o estado atual do conhecimento sobre o tema. Nesse sentido, a análise das normativas nacionais e internacionais relacionadas aos crimes cibernéticos e os princípios constitucionais envolvidos no processo judicial brasileiro permitiu compreender como essas legislações buscam proteger a privacidade e a segurança dos indivíduos, ao mesmo tempo em que enfrentam desafios em acompanhar a evolução constante da tecnologia.

Foram utilizadas também fontes secundárias, como artigos acadêmicos, periódicos, livros e doutrinas especializadas em Direito Digital e Penal, além de publicações de sites institucionais. Essas fontes proporcionaram uma visão aprofundada sobre os conceitos de crimes cibernéticos, segurança digital, e os impactos da Lei Geral de Proteção de Dados (LGPD), da Lei Carolina Dieckmann e da Lei de *Stalking* nos processos judiciais. A partir dessa revisão abrangente, construiu-se um embasamento teórico robusto, essencial para a análise crítica e a formulação das hipóteses relacionadas à eficácia do sistema judiciário brasileiro no enfrentamento dos crimes digitais.

A metodologia adotada visou garantir uma análise detalhada dos aspectos legais e doutrinários envolvidos nos crimes cibernéticos, com foco nas adaptações e desafios que o sistema judiciário enfrenta para aplicar essas leis. A pesquisa permitiu identificar as lacunas e

as necessidades de atualização na legislação brasileira, além das implicações dessas mudanças para a segurança digital e a proteção dos direitos fundamentais dos cidadãos.

DISCUSSÕES E RESULTADOS

Os avanços tecnológicos, em especial o desenvolvimento da *internet*, têm transformado profundamente o comportamento humano, trazendo conveniência e simplicidade. No entanto, esses benefícios também trazem riscos substanciais à segurança digital. A *internet* se tornou um terreno fértil para o surgimento de crimes cibernéticos, que vão desde a invasão de sistemas até o roubo de dados pessoais e financeiros. Diante desse cenário, este estudo buscou analisar a prática dos crimes cibernéticos e identificar as dificuldades enfrentadas pelo sistema judiciário brasileiro para combatê-los de forma eficaz.

A revisão de literatura realizada mostra que, apesar das inovações legislativas, como a Lei Carolina Dieckmann (Lei nº 12.737/2012) e o Marco Civil da Internet (Lei nº 12.965/2014), o Brasil ainda encontra grandes dificuldades para combater esses crimes, sendo demonstrada principalmente suas ineficiências.

Isso se deve, em grande parte, à complexidade técnica envolvida, à rápida evolução dos métodos utilizados pelos criminosos e à carência de profissionais especializados na investigação de delitos cibernéticos. As leis vigentes, embora importantes, são insuficientes para lidar com a amplitude e sofisticação dos crimes digitais, o que compromete a efetividade do direito penal.

Além das lacunas legislativas, outro grande obstáculo identificado é a falta de conscientização da população em relação à segurança digital. Muitos usuários não tomam as medidas necessárias para proteger suas informações pessoais e financeiras, o que facilita a ação dos criminosos.

A educação digital ainda é limitada, tanto no âmbito pessoal quanto institucional, o que contribui para a vulnerabilidade cibernética de uma grande parcela da sociedade. Assim, a conscientização pública é fundamental para a prevenção desses crimes, reforçando a importância de campanhas educativas sobre segurança na *internet*.

Outro ponto destacado pela pesquisa é a necessidade de uma maior cooperação internacional para o combate aos crimes cibernéticos. Como esses crimes geralmente envolvem múltiplas jurisdições, a colaboração entre países é essencial para que as investigações sejam eficazes. O Brasil ainda enfrenta desafios nesse sentido, especialmente em relação à harmonização de legislações e à troca de informações entre autoridades de diferentes nações.

Portanto, embora o Brasil tenha dado passos importantes para criminalizar e combater os crimes cibernéticos, ainda há muito a ser feito para enfrentar a complexidade desses delitos. A melhoria das legislações, a capacitação de profissionais especializados e a conscientização da população são medidas essenciais para reduzir a ocorrência desses crimes.

Somente com uma abordagem integrada, que combine avanços legislativos, cooperação internacional e educação digital, será possível criar um ambiente virtual mais seguro, equilibrando os direitos individuais e a segurança coletiva, considerando que o Estado evolua tanto quanto as tecnologias e seus meios.

CONSIDERAÇÕES FINAIS

Este trabalho teve como foco compreender a dinâmica dos crimes cibernéticos, investigando como esses delitos são cometidos, os métodos e ferramentas utilizados pelos criminosos, bem como as complexidades e barreiras envolvidas na sua investigação e combate. O estudo aprofundou-se nos processos investigativos aplicados a crimes virtuais, identificando as limitações legais, técnicas e institucionais que dificultam a obtenção de provas e a responsabilização dos infratores.

Além disso, analisou as dificuldades enfrentadas por autoridades e profissionais da área, como a falta de infraestrutura adequada, a escassez de especialistas em cibersegurança e as limitações da legislação atual para acompanhar o rápido avanço da tecnologia. O objetivo central do estudo foi, portanto, examinar os principais desafios para enfrentar os crimes virtuais de forma eficaz e propor reflexões sobre possíveis melhorias nas políticas de segurança e nas estratégias de cooperação nacional e internacional.

A justificativa do estudo foi destacar os desafios enfrentados pelas autoridades no processo de investigação dos crimes cometidos via tecnologia, como a falta de legislação específica, a escassez de delegacias especializadas e a carência de profissionais capacitados. Para isso, a pesquisa foi realizada através de uma revisão bibliográfica qualitativa, baseada em leituras e análises de artigos científicos, livros e diversos textos.

A *internet* transformou nossas vidas e formas de comunicação, conectando milhões de pessoas globalmente. Contudo, com essa crescente dependência da tecnologia, surgiram os desafios dos crimes cibernéticos, que afetam indivíduos, empresas e governos. Leis como a Lei Carolina Dieckmann, o Marco Civil da Internet e a Lei Geral de Proteção de Dados refletem os esforços do Brasil para enfrentar essa questão complexa.

Concluiu-se que a investigação de crimes cibernéticos enfrenta obstáculos como a falta de capacitação e dificuldades na coleta de provas. A colaboração entre diversas entidades, como autoridades policiais e o Ministério Público, é essencial para prevenir e reprimir esses crimes. A adesão do Brasil à Convenção de Budapeste fortalece o combate aos crimes cibernéticos, facilitando uma cooperação internacional mais eficiente na investigação e punição dos infratores. Além disso, a educação digital é crucial para prevenir esses crimes, conscientizando os cidadãos sobre os riscos cibernéticos e promovendo práticas seguras na *internet*.

Em síntese, os crimes cibernéticos são uma realidade complexa e em constante evolução, que requer ações coordenadas em diversas frentes. Legislação adequada, capacitação profissional e conscientização pública são elementos essenciais para proteger a sociedade dessas ameaças digitais. A luta contra o crime virtual só será eficaz se compreendermos sua essência. É, portanto, fundamental que as pessoas reconheçam os riscos, saibam como identificá-los e estejam informadas sobre os recursos disponíveis para lidar com esses ataques.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil.** Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 set. 2024.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Dispõe sobre o Código de Processo Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/DecretoLei/Del3689.htm. Acesso em: 14 jul. 2024.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023.** Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato20232026/2023/decreto/d11491.htm. Acesso em: 04 jun. 2024.

BRASIL. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940.** Dispõe sobre o Código Penal Brasileiro. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm. Acesso em: 15 mar. 2024.

BRASIL. **Lei nº 12.737, 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, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 04 jun. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 ago. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/l13709.htm. Acesso em: 04 jun. 2024.

BRASIL. **Lei nº 14.132, de 31 de março de 2021.** Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Brasília, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato20192022/2021/lei/l14132.htm. Acesso em: 04 jun. 2024.

BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013.

CASTRO, Aldemario Araujo. **A internet e os tipos penais que reclamam ação criminosa em público.** 2012. Disponível em: http://egov.ufsc.br/portal/sites/default/files/anexos/1330813309-1-PB.pdf. Acesso em: 14 jun. 2024.

CRESPO, Marcelo. **Algumas reflexões sobre o cyberstalking.** JusBrasil. 2015. Disponível em: https://www.jusbrasil.com.br/artigos/algumas-reflexoes-sobre-ocyberstalking/226885184. Acesso em: 11 jun. 2024.

CRUZ, Rogerio Schietti. **Conflito de Competência nº 136.700 - SP (2014/0274368-9)**. Brasilia (DF). STJ. 23/09/2015. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=52822191&tipo=5&nreg=201402743689&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20151001&formato=PDF&salvar=false. Acesso em: 14 jun. 2024

CUNHA, Rogério Sanches. **Lei nº14.132/21: insere no código penal o artigo 147-a para tipificar o crime de perseguição**. Meu Site Jurídico. 2021. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/04/01/lei-14-13221-insere-no-codigopenal-o-art-147-para-tipificar-o-crime-de-perseguicao/. Acesso em: 20 set. 2024.

GALLI, Marcelo. **Consultor Jurídico.** Disponível em: https://www.conjur.com.br/2017-mai26/direito-nao-preparado-enfrentar-crime-digital-schietti/. Acesso em: 14 mar. 2024.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 6ª ed. São Paulo: Atlas, 2019.

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

LIMA, Leandro. **Cyrela é a 1a empresa a violar a LGPD e ser condenada**. NowCy. 2022. Disponível em: https://nowcy.com.br/cyrela-e-a-1a-empresa-a-violar-a-lgpd-e-sercondenada/. Acesso em: 15 jun. 2024.

MICOLI, Alessia. **Il Fenomeno Dello Stalking.** Aspetti giuridici e psicologici. Milão: Giuffrè, 2012.

NASCIMENTO, Samir Paula. **Cibercrime:** Conceitos, modalidades e aspectos jurídicospenais. 2019. Disponível em: https://ambitojuridico.com.br/cadernos/internet-einformatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/. Acesso em: 05 jul. 2024.

OTHON, Dante Pessoa; DAMASCENO, Ingrid Maria Santos das Neves. **Crimes cibernéticos: desafios enfrentados no processo investigatório**. 2023. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/34915. Acesso em: 12 jul. 2024.

PAIVA, Leticia. **LGPD**: **77% das decisões não resultaram em condenação em 2021**. Disponível em: https://www.jota.info/justica/lgpd-condenacao-77-das-decisoes-nao. Acesso em: 14 jul. 2024.

TEIXEIRA, T. **Direito digital e processo eletrônico.** 7. ed. São Paulo: Saraiva, 2023. Ebook.