O CRESCIMENTO DOS CRIMES CIBERNÉTICOS E DO ESTELIONATO VIRTUAL NO BRASIL

THE GROWTH OF CYBER CRIMES AND VIRTUAL SCAMMERS IN BRAZIL

Rubens Matheus Garcia Barros
Graduando (a) do Curso de Direito do Centro Universitário São Jose.

Orientador
Prof. Sérgio Mouta.

RESUMO

Este estudo tem como objetivo geral analisar a evolução dos crimes cibernéticos no Brasil, bem como a evolução da legislação no combate a tais delitos, destacando a importância de uma abordagem legal atualizada para lidar com os desafios do mundo virtual. Para tanto, a pesquisa baseia-se em uma abordagem de pesquisa bibliográfica, que envolve a análise crítica de literatura acadêmica, legislação e documentos relacionados aos crimes cibernéticos e à evolução das leis penais no âmbito virtual. A coleta e análise de dados foram realizadas mediante revisão sistemática de fontes confiáveis e atualizadas. A crescente incidência de crimes cibernéticos e a rápida evolução tecnológica destacam a necessidade de uma legislação penal adequada para lidar com esses desafios. A proteção dos direitos dos cidadãos e a garantia da segurança cibernética são imperativos em um mundo cada vez mais digitalizado. Este estudo busca contribuir para o entendimento das mudanças na legislação penal brasileira relacionadas aos crimes cibernéticos, evidenciando a importância da atualização constante das leis para manter a sociedade segura e protegida no ambiente virtual. Além disso, pretende-se destacar como essas mudanças refletem os princípios fundamentais de justiça e privacidade no contexto digital, promovendo uma reflexão sobre o equilíbrio entre a repressão dos delitos cibernéticos e a proteção dos direitos individuais.

Palavras-chave: Crimes Digitais, Internet e Legislação Penal.

ABSTRACT

This study's general objective is to analyze the evolution of cybercrimes in Brazil, as well as the evolution of legislation to combat such crimes, highlighting the importance of an updated legal approach to dealing with the challenges of the virtual world. To this end, the research is based on a bibliographical research approach, which involves the critical analysis of academic literature, legislation and documents related to cybercrimes and the evolution of criminal laws in the virtual sphere. Data collection and analysis were carried out through a systematic

review of reliable and updated sources. The growing incidence of cybercrimes and rapid technological evolution highlight the need for adequate criminal legislation to deal with these challenges. Protecting citizens' rights and ensuring cybersecurity are imperative in an increasingly digitalized world. This study seeks to contribute to the understanding of changes in Brazilian criminal legislation related to cybercrimes, highlighting the importance of constantly updating laws to keep society safe and protected in the virtual environment. Furthermore, it is intended to highlight how these changes reflect the fundamental principles of justice and privacy in the digital context, promoting a reflection on the balance between the repression of cybercrimes and the protection of individual rights.

Keywords: Digital Crimes, Internet, Criminal Legislation.

INTRODUÇÃO

Nos últimos anos, a sociedade testemunhou uma revolução digital que transformou a maneira como se vive, trabalha e os meios de comunicação. A internet e as tecnologias digitais trouxeram inúmeras oportunidades, conectando pessoas em todo o mundo e impulsionando o progresso em diversos setores. No entanto, essa transformação também deu origem a uma série de desafios e ameaças, com o surgimento de crimes cibernéticos que exploram as vulnerabilidades do ambiente virtual. Nesse contexto, a evolução da legislação penal tornou-se essencial para combater eficazmente os delitos no âmbito virtual e garantir a segurança cibernética.

A partir disso, o objetivo geral deste estudo é analisar o crescimento dos crimes virtuais no Brasil, bem como a evolução da legislação penal no combate a tais delitos, destacando as principais leis e regulamentos que foram promulgados no Brasil para lidar com essa crescente ameaça. Pretende-se compreender como as leis têm evoluído ao longo do tempo para enfrentar os desafios do mundo digital e promover a proteção dos direitos dos cidadãos no ambiente virtual.

Para alcançar o objetivo proposto, esta pesquisa será conduzida por meio de uma abordagem baseada em pesquisa bibliográfica. A pesquisa bibliográfica é um método amplamente reconhecido e utilizado na academia, que envolve a busca e análise crítica de fontes bibliográficas, como livros, artigos científicos, legislação, jurisprudência e documentos governamentais relacionados ao tema em questão. Essa metodologia permitirá uma investigação aprofundada da evolução da legislação penal no contexto dos crimes cibernéticos.

A escolha deste tema se justifica pela crescente importância dos crimes cibernéticos na sociedade contemporânea. Com o avanço da tecnologia e a digitalização de diversos aspectos de nossas vidas, as ameaças cibernéticas se tornaram uma preocupação cotidiana. Desde ataques

cibernéticos a sistemas críticos até estelionatos virtuais que afetam indivíduos, os crimes digitais têm o potencial de causar danos significativos.

Além disso, a falta de regulamentação adequada no início da era digital deixou uma lacuna na proteção dos cidadãos contra ameaças virtuais. À medida que a internet se expandia, surgia a necessidade de leis que abordassem essas novas formas de delinquência. A legislação penal precisava evoluir para acomodar a complexidade e a dinâmica do ciberespaço.

A justificativa para este estudo também reside na importância de se compreender como a legislação penal brasileira tem respondido aos desafios da cibercriminalidade. A análise da evolução das leis relacionadas a crimes cibernéticos permitirá avaliar o progresso e as lacunas na proteção cibernética, bem como identificar áreas que requerem maior atenção e desenvolvimento legislativo.

Portanto, o conhecimento sobre as leis e regulamentos relacionados a crimes digitais é fundamental para advogados, agentes da lei, acadêmicos, legisladores e todos os que buscam compreender e enfrentar eficazmente a cibercriminalidade. O estudo também contribui para a conscientização pública sobre os direitos e responsabilidades dos cidadãos no ambiente virtual.

1. FUNDAMENTAÇÃO TEÓRICA

No contexto da sociedade moderna, cada vez mais digitalizada, os crimes cibernéticos têm se tornado uma preocupação crescente para governos, empresas e indivíduos. Esses crimes, cometidos por meio de dispositivos eletrônicos e da internet, abrangem uma ampla gama de atividades ilícitas, como fraudes eletrônicas, roubo de identidade, invasões de sistemas e disseminação de malware. A sua natureza complexa e transnacional representa um desafio significativo para as autoridades e para o sistema jurídico.

Definir e compreender as características dos crimes cibernéticos é fundamental para a implementação de estratégias eficazes de prevenção e repressão. Segundo Almeida (2018, p.107), "os crimes cibernéticos são condutas delitivas praticadas por meio do uso de tecnologias de informação e comunicação, nas quais o meio digital é utilizado como instrumento para a prática de infrações penais". Essas infrações podem envolver desde o acesso não autorizado a sistemas e a obtenção de informações confidenciais até a disseminação de conteúdos ofensivos ou prejudiciais.

Assim, a definição de crimes cibernéticos é ampla e abrange uma variedade de condutas delitivas praticadas por meio da utilização de tecnologias da informação e comunicação. Os crimes cibernéticos são condutas delitivas que ocorrem por meio do uso de tecnologias de informação e comunicação, onde o meio digital é utilizado como instrumento para a prática de infrações penais. Esses delitos são cometidos de maneira virtual, envolvendo a utilização de dispositivos eletrônicos e a internet para a realização de atividades ilegais. Com o avanço tecnológico e a ampla adoção da internet em diversas esferas da sociedade, os crimes cibernéticos se tornaram uma preocupação global. (ALMEIDA, 2018).

Uma das principais características dos crimes cibernéticos é a sua natureza transnacional. Devido à capacidade de conexão global proporcionada pela internet, os criminosos podem operar em qualquer lugar do mundo, ultrapassando fronteiras físicas e dificultando a identificação e a punição dos responsáveis. Conforme aponta Kshetri (2017, p.144), "os crimes cibernéticos não estão restritos a uma jurisdição específica, e os criminosos podem operar virtualmente de qualquer lugar, dificultando a cooperação internacional e a aplicação da lei".

Segundo Rabelo (2020, p.144), "os crimes cibernéticos não estão vinculados a uma localização geográfica específica, o que dificulta a identificação e a punição dos infratores, bem como a cooperação internacional na investigação desses delitos".

Outra característica dos crimes cibernéticos é a utilização de técnicas e ferramentas específicas. Os criminosos cibernéticos se valem de métodos sofisticados para obter acesso indevido a sistemas, roubar informações confidenciais, disseminar malware, realizar fraudes e outras atividades ilícitas. Essas técnicas podem incluir a engenharia social, que envolve a manipulação psicológica das vítimas para obter informações ou acesso a sistemas, e a exploração de vulnerabilidades em softwares e redes.

Uma das formas mais comuns de crimes cibernéticos é o phishing, que consiste em tentativas de obtenção de informações confidenciais, como senhas e dados bancários, por meio de e-mails, mensagens ou sites falsos que se assemelham aos legítimos. Esse tipo de crime se baseia na engenharia social e na persuasão dos usuários a revelarem informações pessoais. Além disso, os criminosos também podem utilizar ransomware, que é um tipo de malware que bloqueia o acesso aos sistemas ou criptografa arquivos, exigindo um resgate para sua liberação.

Outra característica dos crimes cibernéticos é a dificuldade na identificação dos infratores. O anonimato proporcionado pelo ambiente digital torna desafiador rastrear e responsabilizar os

criminosos. Conforme apontado por Santos (2019, p.125), "a natureza virtual dos crimes cibernéticos dificulta a identificação dos infratores, uma vez que eles podem ocultar sua verdadeira identidade por meio de técnicas de anonimato e uso de servidores proxy". Essa falta de identificação dificulta a aplicação das leis e a responsabilização dos infratores.

A diversidade dos tipos de crimes cibernéticos é outro fator importante de ser mencionado. Esses delitos podem abranger uma ampla gama de atividades ilegais, incluindo, mas não se limitando a: fraudes eletrônicas, como phishing e esquemas de pirâmide; roubo de identidade, envolvendo a obtenção e utilização indevida de informações pessoais; invasão de sistemas, com o objetivo de acesso não autorizado a computadores e redes; disseminação de malware, incluindo vírus, worms e ransomware; crimes contra a propriedade intelectual, como pirataria e violação de direitos autorais (REDDY, 2018).

Além da diversidade de crimes, os crimes cibernéticos também apresentam algumas características particulares em relação aos crimes tradicionais. Um desses aspectos é a velocidade e a facilidade com que os crimes podem ser cometidos. Os criminosos cibernéticos podem realizar suas atividades em questão de minutos, explorando as vulnerabilidades dos sistemas e as deficiências de segurança. Segundo Holt e Bossler (2017, p.198), "os crimes cibernéticos podem ser cometidos rapidamente, permitindo que os criminosos obtenham ganhos financeiros e evitem a detecção antes que as vítimas percebam o que aconteceu".

A complexidade técnica dos crimes cibernéticos é mais uma característica relevante. Os infratores cibernéticos geralmente possuem habilidades avançadas em informática e conhecimento técnico para explorar vulnerabilidades e desenvolver técnicas sofisticadas. Essa complexidade exige o uso de especialistas em segurança cibernética e a cooperação entre diferentes entidades, como governos, empresas e organizações internacionais, para combater esses delitos (REDDY, 2018).

Por fim, a falta de fronteiras jurisdicionais claras e a ausência de uma estrutura legal internacional abrangente são características que dificultam a repressão efetiva dos crimes cibernéticos. Os delitos cometidos na internet podem envolver indivíduos de diferentes países, levantando questões de competência legal e cooperação internacional. A ausência de um quadro jurídico internacional unificado para enfrentar os crimes cibernéticos tem sido um desafio para as autoridades em todo o mundo (HOLT; BOSSLER, 2017).

Além disso, os crimes cibernéticos são caracterizados por sua abrangência e impacto significativo na sociedade moderna. Esses crimes afetam não apenas indivíduos, mas também empresas, organizações governamentais e até mesmo países inteiros. As consequências podem variar desde prejuízos financeiros, como roubo de informações bancárias e fraudes eletrônicas, até violações de privacidade, disseminação de informações falsas, comprometimento da segurança nacional e danos à reputação de pessoas e instituições.

Portanto, os crimes cibernéticos são condutas delitivas praticadas por meio de tecnologias da informação e comunicação, em que o meio digital é utilizado como instrumento para a prática de infrações penais. Caracterizam-se pela transnacionalidade, utilização de técnicas e ferramentas específicas, dificuldade na identificação dos infratores e impacto significativo na sociedade moderna. O entendimento dessas definições e características é fundamental para a implementação de estratégias eficazes de prevenção e combate a esses crimes.

2. CORPO DO TRABALHO/DESENVOLVIMENTO

O avanço da tecnologia e a popularização da internet trouxeram inúmeras facilidades para a sociedade moderna, mas também abriram espaço para novas formas de criminalidade. Nesse contexto, o estelionato virtual desponta como uma modalidade criminosa que tem se destacado pela sua sofisticação e capacidade de atingir um grande número de vítimas.

A definição do estelionato virtual encontra-se no artigo 171 do Código Penal Brasileiro, que trata do estelionato em geral. Contudo, no ambiente virtual, as práticas criminosas ganham novas roupagens e estratégias. Uma das formas mais comuns de estelionato virtual é a criação de sites falsos, que se assemelham a páginas legítimas de bancos, lojas virtuais ou órgãos governamentais, com o intuito de obter informações confidenciais das vítimas, como senhas bancárias, dados de cartões de crédito e documentos pessoais. Esse tipo de golpe é conhecido como "phishing" (ROXIN, 2008).

O phishing é uma técnica que explora a ingenuidade e a falta de conhecimento de alguns usuários em relação aos riscos da internet. Por meio de e-mails ou mensagens enviadas em aplicativos de comunicação, os criminosos se passam por instituições confiáveis e solicitam informações pessoais dos usuários. Ao clicar em links maliciosos ou fornecer dados pessoais em páginas falsas, as vítimas acabam sendo enganadas e têm suas informações comprometidas.

Outra modalidade de estelionato virtual é o golpe do falso suporte técnico. Nessa prática, os criminosos entram em contato com as vítimas, geralmente por telefone, fazendo-se passar por funcionários de empresas de tecnologia ou provedores de internet. Sob o pretexto de oferecer auxílio técnico, os golpistas solicitam acesso remoto ao computador das vítimas, o que lhes permite instalar malwares, roubar informações pessoais ou até mesmo exigir pagamento por serviços inexistentes (MIRABETE; FABBRINI, 2017).

Além disso, o estelionato virtual também se manifesta em outros formatos, como a venda de produtos falsificados ou inexistentes em plataformas de comércio eletrônico, o oferecimento de oportunidades de investimento falsas em criptomoedas ou outros esquemas de pirâmide, e a aplicação de golpes em redes sociais, onde os criminosos se passam por pessoas conhecidas das vítimas para solicitar dinheiro ou informações pessoais.

É importante ressaltar que o estelionato virtual pode ser praticado por indivíduos ou organizações criminosas, muitas vezes com atuação internacional, o que dificulta a investigação e a punição dos responsáveis. A natureza intangível do ambiente virtual e as dificuldades em rastrear os autores desses golpes demandam uma ação coordenada e eficiente das autoridades e dos órgãos de segurança (SCHUNEMANN, 2010).

As consequências do estelionato virtual para as vítimas são diversas e impactantes. Além do prejuízo financeiro, que pode ser significativo, há também o dano emocional e psicológico decorrente da violação da privacidade e da sensação de vulnerabilidade e insegurança. Muitas vítimas se sentem envergonhadas e relutam em reportar o crime às autoridades, o que dificulta a obtenção de dados para as investigações e a responsabilização dos criminosos.

Diante desse cenário, a prevenção e o combate ao estelionato virtual se tornam fundamentais para garantir a segurança dos usuários da internet. A conscientização sobre os riscos e as técnicas utilizadas pelos golpistas é uma das principais medidas preventivas. Educar a população sobre os perigos do phishing, da instalação de softwares de fontes desconhecidas e da divulgação de informações pessoais em redes sociais pode reduzir significativamente a ocorrência desses crimes.

Além disso, a implementação de mecanismos de segurança cibernética por parte das empresas de tecnologia e instituições financeiras é essencial para evitar a disseminação de páginas falsas e a obtenção indevida de informações dos usuários. A atualização constante dos sistemas de segurança, a verificação rigorosa de transações suspeitas e o monitoramento de

atividades suspeitas são algumas das ações que podem contribuir para a proteção dos usuários contra os golpes virtuais (BITENCOURT, 2019).

No âmbito jurídico, é necessário o aprimoramento da legislação para enfrentar o estelionato virtual, considerando a dinamicidade e a evolução constante dos crimes cibernéticos. A criação de leis específicas que tipifiquem e punam de forma adequada as práticas criminosas no ambiente virtual é um passo importante para a efetividade do combate a esse tipo de crime. Além disso, é essencial a capacitação dos profissionais da área jurídica e dos órgãos de segurança no tratamento de crimes cibernéticos, possibilitando uma resposta rápida e eficaz diante dos golpes virtuais.

Portanto, o estelionato virtual é uma forma de crime que tem se tornado cada vez mais presente e sofisticada com o avanço da tecnologia. Os criminosos se utilizam de técnicas enganosas e fraudes para obter vantagem ilícita em prejuízo de suas vítimas, explorando a vulnerabilidade e a falta de conhecimento de alguns usuários. A prevenção e o combate ao estelionato virtual requerem uma ação integrada entre governos, empresas de tecnologia, instituições financeiras e a sociedade como um todo. A conscientização sobre os riscos, a implementação de mecanismos de segurança cibernética e o aprimoramento da legislação são medidas fundamentais para proteger os usuários da internet e garantir a integridade e a confiança no ambiente virtual. O enfrentamento do estelionato virtual é um desafio que demanda esforços contínuos e articulados, visando a preservação da segurança e a promoção de uma cultura digital mais segura e responsável.

2.1 A evolução da legislação brasileira no combate aos crimes cibernéticos

A evolução da legislação brasileira no combate aos crimes cibernéticos é um tema de extrema relevância no contexto atual, em que a tecnologia digital desempenha um papel cada vez mais central em nossas vidas. Com o crescimento exponencial da internet e o aumento do acesso a diversas informações, os crimes cometidos no ambiente virtual tornaram-se cada vez mais frequentes. Como destacado por Silva (2020, p. 45), "a tecnologia trouxe inúmeras oportunidades, mas também desafios, e um deles é o aumento dos crimes cibernéticos."

A rápida evolução tecnológica e a aceleração dos delitos cibernéticos têm gerado uma sensação de impunidade entre aqueles que não se sentem devidamente protegidos legalmente. Como ressalta Rocha (2018, p. 72), "a sensação de impunidade é um dos principais incentivos

para a prática de crimes cibernéticos, uma vez que a complexidade desses delitos muitas vezes dificulta a investigação e a responsabilização dos infratores."

No entanto, o mundo digital não pode ser um refúgio seguro para atos criminosos. É nesse contexto que a evolução das leis brasileiras desempenha um papel crucial na repressão e prevenção desses tipos de delitos. Como argumenta Lima (2019, p. 88), "a legislação deve acompanhar as transformações da sociedade e do ambiente digital, a fim de proteger os direitos e garantias dos cidadãos."

Um dos marcos mais importantes nessa transformação é a Lei dos Crimes Cibernéticos, conhecida como Lei Carolina Dieckman, de número 12.737/2012. Esta lei trouxe importantes avanços no combate aos crimes cibernéticos, criminalizando a invasão de dispositivos eletrônicos e a divulgação não autorizada de informações pessoais. Segundo Fonseca (2017, p. 53), "a Lei Carolina Dieckman foi um passo fundamental para tornar mais efetiva a punição dos infratores digitais e aumentar a proteção da privacidade online."

Outro marco significativo é o Marco Civil da Internet, estabelecido pela Lei 12.965/2014. Esta legislação trouxe uma série de direitos e deveres para os usuários da internet no Brasil, bem como estabeleceu princípios fundamentais para a proteção da neutralidade da rede e da privacidade dos usuários. De acordo com Santos (2016, p. 105), "o Marco Civil da Internet representa um avanço significativo na regulamentação da internet no Brasil, garantindo direitos importantes para os usuários e estabelecendo limites para a atuação das empresas de tecnologia."

Além disso, a Lei Geral de Proteção de Dados (LGPD), de número 13.709/2018, desempenha um papel fundamental na proteção dos dados pessoais dos cidadãos. Essa legislação estabelece regras rígidas para a coleta, armazenamento e tratamento de informações pessoais por parte das empresas e organizações que atuam no ambiente digital. De acordo com Oliveira (2020, p. 67), "a LGPD é um importante instrumento para garantir a privacidade e a segurança dos dados dos usuários, mitigando os riscos de vazamentos e uso indevido das informações pessoais."

Vale também destacar a Lei 14.155/2021, que trouxe agravamento das penas para os crimes de invasão de dispositivos, furto qualificado e estelionato ocorridos em meio digital, conectado ou não à internet. Como afirmou Souza (2021, p. 29), "essa lei representa um passo adiante na repressão dos crimes cibernéticos, tornando as punições mais severas e desencorajando os infratores."

A constante evolução do ordenamento jurídico brasileiro no combate aos crimes cibernéticos reflete a necessidade de adaptação às mudanças na sociedade e no ambiente digital. Como argumenta Ribeiro (2019, p. 114), "as leis precisam acompanhar o ritmo das inovações tecnológicas e proteger os direitos dos cidadãos na era digital."

Nesse sentido, as modificações legislativas não podem ser vistas como meios livres para a prática de atos que prejudicam a sociedade e violam suas garantias conquistadas ao longo do tempo. O retrocesso não é apenas inadequado, mas também deve ser combatido em todos os espaços necessários. Como ressalta Silva (2020, p. 58), "a sociedade democrática depende de um ordenamento jurídico que esteja à altura dos desafios da era digital, protegendo os direitos e interesses de todos os cidadãos."

Assim, a evolução da legislação brasileira no combate aos crimes cibernéticos é uma resposta necessária às transformações na sociedade e na tecnologia. As leis mencionadas, como a Lei Carolina Dieckman, o Marco Civil da Internet, a LGPD e a Lei 14.155/2021, desempenham um papel fundamental na proteção dos direitos e garantias dos cidadãos na era digital. Ao longo desta seção, explorar-se-á com mais detalhes o impacto dessas leis na repressão e prevenção dos crimes cibernéticos, bem como os desafios que ainda persistem nesse campo.

2.2 A lei dos crimes cibernéticos (lei nº 12.737/2012) - O caso Carolina Dieckman

A Lei nº 12.737/2012, também conhecida como Lei Carolina Dieckmann, é um marco importante na legislação brasileira que trata dos crimes cibernéticos. Tal diploma fora promulgado em 30 de novembro de 2012 e entrou em vigor em 2 de abril de 2013. Sua criação foi motivada por uma série de incidentes de invasão de privacidade e compartilhamento não autorizado de conteúdo pessoal na internet.

O caso Carolina Dieckmann, uma renomada atriz brasileira, ganhou destaque nacional e internacional em 2012. Carolina teve fotos íntimas pessoais roubadas de seu computador e posteriormente divulgadas na internet. Isso levou a uma discussão intensa sobre a falta de regulamentação e proteção contra essas violações no ambiente digital.

A Lei 12.737/2012 abordou questões relacionadas à invasão de dispositivos eletrônicos e à divulgação não autorizada de conteúdo pessoal na internet. Apresentou uma série de definições e penalidades para crimes cibernéticos, incluindo:

a) **Invasão de Dispositivos (Art. 154-A):** A lei tornou crime a invasão de dispositivos eletrônicos alheios, como computadores e smartphones, sem autorização. O infrator pode enfrentar pena de detenção de até um ano e multa.
b) **Obtenção, Transferência ou Compartilhamento de Dados (Art. 154-B):** A obtenção, transferência ou compartilhamento não autorizado de dados pessoais também foi criminalizado pela lei, sujeitando o infrator a penalidades semelhantes à invasão de dispositivos.
c) **Divulgação de Conteúdo Íntimo sem Autorização (Art. 216-B):** A divulgação não autorizada de material íntimo de outra pessoa na internet tornou-se crime. A pena pode variar de um a cinco anos de prisão, dependendo da gravidade do caso.

Além disso, a Lei dos Crimes Cibernéticos trouxe mudanças significativas no tratamento legal dos crimes cibernéticos no Brasil. Ela representou um esforço importante para proteger a privacidade e a segurança dos cidadãos no ambiente digital. No entanto, sua implementação e aplicação não estão isentas de desafios.

Segundo Fonseca (2017) a lei poderia ser mais abrangente e atualizada para abordar novas formas de crimes cibernéticos que surgiram desde sua promulgação. Em um estudo publicado em 2018, Barreto e Santana destacaram a necessidade de adaptação constante da legislação devido à rápida evolução da tecnologia e das táticas criminosas na internet. Os autores afirmam: "As leis devem ser flexíveis o suficiente para acomodar novos desafios e ameaças que emergem na era digital." (BARRETO; SANTANA, 2018, p. 55)

Além disso, a eficácia da lei também depende da capacidade das autoridades de aplicá-la adequadamente. Em muitos casos, a investigação e a identificação dos infratores ainda são desafios complexos no ambiente cibernético, onde a anonimidade pode ser facilmente preservada.

Portanto, a Lei dos Crimes Cibernéticos, desempenha um papel crucial na regulamentação e punição de atividades criminosas no ambiente digital. Ela foi promulgada em resposta ao notório caso de invasão de privacidade envolvendo a atriz Carolina Dieckmann. A lei definiu penalidades para a invasão de dispositivos eletrônicos, obtenção não autorizada de dados e divulgação não autorizada de conteúdo pessoal.

No entanto, a evolução rápida da tecnologia e das táticas criminosas na internet levanta questões sobre a necessidade de constante adaptação da legislação para lidar com novos desafios.

Além disso, a eficácia da lei depende da capacidade das autoridades de aplicá-la efetivamente em um ambiente cibernético complexo e em constante mudança. A Lei Carolina Dieckmann representa um passo importante na proteção dos direitos dos cidadãos no mundo digital, mas ainda há muito trabalho a ser feito para garantir a segurança e a privacidade online.

2.3 O marco civil da internet (lei nº 12.965/2014) e a proteção de dados dos usuários

O Marco Civil da Internet, também conhecido como Lei 12.965/2014, representa um marco regulatório fundamental no cenário da governança da internet no Brasil. Promulgado em 23 de abril de 2014, este conjunto de princípios e diretrizes estabelece os fundamentos legais para o uso da internet no país. Entre seus principais objetivos está a promoção da liberdade de expressão, privacidade e neutralidade da rede, bem como o estabelecimento de diretrizes para a responsabilidade dos provedores de serviços. Neste contexto, essa seção se concentrará em analisar as garantias proporcionadas pelo Marco Civil da Internet em relação à neutralidade da rede, proteção de dados pessoais e responsabilidade dos provedores de serviços.

A neutralidade da rede é um dos princípios fundamentais do Marco Civil da Internet e desempenha um papel crucial na manutenção da igualdade no acesso à internet. Conforme estabelecido no artigo 3º, II, do Marco Civil, a neutralidade da rede garante que o tratamento dos dados trafegados na internet seja isonômico, sem discriminação quanto ao conteúdo, origem, destino ou serviço utilizado. Para entender melhor essa garantia, é relevante citar o jurista Sergio Amadeu da Silveira, que argumenta que:

A neutralidade da rede é uma condição essencial para a democracia digital, pois garante que a internet continue a ser um espaço de livre circulação de informações e de igualdade de oportunidades para todos os serviços e aplicações. (SILVEIRA, 2015)

A neutralidade da rede impede que provedores de serviços de internet (ISPs) priorizem determinados tipos de tráfego, bloqueiem ou reduzam a velocidade de acesso a serviços ou aplicativos específicos em favor de outros. Isso garante que todos os conteúdos e serviços online tenham a mesma chance de serem acessados, independentemente de sua origem ou natureza.

Outra garantia fundamental do Marco Civil da Internet é a proteção de dados pessoais, que está intrinsecamente relacionada à privacidade dos usuários online. De acordo com o artigo 3º, VII, do Marco Civil, o tratamento de dados pessoais deve ocorrer de acordo com a lei e com o consentimento expresso do titular dos dados. A lei nº 13.709/2018, conhecida como Lei Geral de

Proteção de Dados (LGPD), complementa essa proteção, estabelecendo diretrizes mais detalhadas para o tratamento de dados pessoais.

Nesse contexto, vale citar a contribuição de Danilo Doneda (2019, p.123), autor renomado na área de proteção de dados no Brasil, que afirma: "A proteção de dados pessoais é um elemento essencial para a confiança dos usuários na internet, pois permite que eles tenham controle sobre suas informações e saibam como elas são utilizadas."

A proteção de dados pessoais no Marco Civil da Internet e na LGPD visa garantir que os dados dos usuários sejam tratados de forma transparente e segura, com o mínimo de interferência em sua privacidade. Isso inclui a necessidade de consentimento explícito para coleta e uso de dados, bem como a obrigação de empresas e provedores de serviços de protegerem adequadamente essas informações.

Além disso, o Marco Civil da Internet também estabelece diretrizes importantes relacionadas à responsabilidade dos provedores de serviços online. O artigo 19 do Marco Civil determina que provedores de aplicações de internet não são responsáveis pelo conteúdo gerado por terceiros, a menos que não cumpram uma ordem judicial específica para remoção desse conteúdo. Essa disposição visa equilibrar a liberdade de expressão com a necessidade de proteção contra conteúdos ilícitos.

A respeito dessa questão, Pablo Ortellado (2019, p.65), professor e pesquisador na área de internet e democracia, destaca: "A responsabilidade limitada dos provedores de serviços é essencial para a promoção da liberdade de expressão na internet, uma vez que permite que plataformas online ofereçam um espaço para diferentes vozes e opiniões."

No entanto, a aplicação prática dessa garantia tem gerado debates significativos, especialmente quando se trata da disseminação de desinformação e discurso de ódio online. A definição de limites claros para a responsabilidade dos provedores de serviços continua sendo um desafio importante.

Portanto, o Marco Civil da Internet estabelece um conjunto abrangente de garantias que desempenham um papel fundamental na governança da internet no Brasil. A neutralidade da rede, a proteção de dados pessoais e a responsabilidade dos provedores de serviços são elementos essenciais para a promoção da igualdade de acesso, a privacidade dos usuários e a liberdade de expressão online. No entanto, a eficácia dessas garantias depende da aplicação adequada da lei, bem como da adaptação contínua às transformações digitais em curso. Portanto, é essencial que o

Marco Civil da Internet seja constantemente revisado e aprimorado para enfrentar os desafios emergentes e proteger efetivamente os direitos dos usuários na era digital.

2.4 A lei geral de proteção de dados (lei nº 13.709/2018) e sua importância na era digital

A Lei Geral de Proteção de Dados (LGPD) do Brasil, promulgada em 2018, representa um marco importante na garantia da privacidade e da segurança dos dados dos cidadãos, bem como na regulamentação do tratamento desses dados por parte das organizações.

Tal diploma legal foi inspirada em regulamentações europeias, como o Regulamento Geral de Proteção de Dados (GDPR), e estabelece diretrizes claras para a coleta, o uso, o armazenamento e o compartilhamento de dados pessoais no Brasil. Ela se aplica a todas as empresas e entidades que operam no país, independentemente de sua localização, e impõe obrigações significativas em relação à proteção de dados pessoais.

Um dos aspectos mais importantes da LGPD é o consentimento do titular dos dados. Conforme previsto na lei, as organizações devem obter o consentimento explícito e informado dos indivíduos antes de coletar e processar seus dados pessoais. Isso significa que os usuários têm o direito de saber quais dados estão sendo coletados, para que finalidade, por quanto tempo serão armazenados e com quem serão compartilhados (Artigo 9º, § 2º). (BRASIL, 2018)

A importância do consentimento informado na LGPD é destacada por Doneda (2019), que argumenta que a privacidade não deve ser tratada como um "nada a esconder", mas sim como um direito fundamental. Ele observa que as pessoas têm o direito de saber e controlar como suas informações pessoais estão sendo usadas, o que reforça a ideia de que o consentimento é uma parte crucial da proteção de dados pessoais.

Outro aspecto relevante da LGPD é a criação da figura do Encarregado de Proteção de Dados (DPO), responsável por garantir o cumprimento da lei dentro das organizações. O DPO desempenha um papel fundamental na promoção da conformidade com a LGPD e na proteção dos direitos dos titulares de dados. A existência de um DPO é um dos requisitos para o tratamento de dados pessoais, e sua nomeação demonstra o compromisso da organização com a proteção de dados (Artigo 41). (BRASIL, 2018)

No contexto da era digital, em que a coleta e o uso de dados pessoais são ubíquos, a LGPD desempenha um papel crucial na garantia da privacidade e da segurança dos indivíduos. Como destaca Rezende (2019), a lei proporciona aos cidadãos brasileiros maiores controle sobre

suas informações pessoais, permitindo-lhes tomar decisões informadas sobre a divulgação de seus dados. Isso é particularmente relevante em um cenário em que empresas frequentemente usam dados para personalizar publicidade e serviços, muitas vezes sem o conhecimento ou consentimento adequado dos usuários.

A LGPD também estabelece regras rigorosas para a segurança dos dados pessoais, exigindo que as organizações adotem medidas técnicas e administrativas para proteger essas informações contra acessos não autorizados e vazamentos (Artigo 46). Essa preocupação com a segurança dos dados é crucial em um ambiente digital em constante evolução, em que ameaças cibernéticas são uma realidade constante. (BRASIL, 2018)

Além disso, a LGPD prevê penalidades severas para organizações que não cumprem a lei, incluindo multas que podem chegar a 2% do faturamento anual da empresa, com um limite de até R$ 50 milhões por infração (Artigo 52). Essas penalidades incentivam as organizações a investirem em medidas de proteção de dados e a levarem a sério a conformidade com a lei. (BRASIL, 2018)

É importante destacar que a LGPD não apenas beneficia os indivíduos ao proteger seus dados pessoais, mas também promove a confiança na economia digital. A confiança dos consumidores é fundamental para o crescimento do comércio eletrônico e para o desenvolvimento de serviços digitais. Quando os usuários confiam que suas informações estão sendo tratadas com responsabilidade, eles estão mais propensos a utilizar os serviços online e a se envolver em transações comerciais na internet.

Portanto, a Lei Geral de Proteção de Dados (LGPD) desempenha um papel vital na era digital, garantindo a privacidade, a segurança e a confiança dos indivíduos no ambiente digital. Ao estabelecer regras claras para a proteção de dados pessoais e impor penalidades por não conformidade, a LGPD ajuda a equilibrar o uso da tecnologia com a proteção dos direitos fundamentais dos cidadãos em um mundo cada vez mais interconectado e orientado por dados.

2.5 A lei 14.155/2021 e o agravamento das penas para crimes digitais

A Lei 14.155/2021 foi sancionada em 27 de maio de 2021 e entrou em vigor em agosto do mesmo ano. Seu objetivo principal é tornar mais rigorosa a punição para crimes como invasão de dispositivos, furto qualificado e estelionato, quando cometidos em ambiente digital. Essa lei representa um passo significativo na adequação do ordenamento jurídico brasileiro à realidade da

era digital, considerando que as punições existentes anteriormente não eram suficientes para dissuadir a prática desses crimes.

Um dos aspectos mais relevantes da Lei 14.155/2021 é o agravamento das penas para os crimes digitais. Antes de sua promulgação, os criminosos que atuavam no ambiente virtual muitas vezes enfrentavam penalidades brandas, o que não desencorajava a prática criminosa. Com a nova legislação, as punições se tornaram mais severas, refletindo a gravidade dos delitos cometidos no ambiente digital.

Tal diploma normativo estabelece em seu texto que a invasão de dispositivo informático, seja ele conectado ou não à internet, com o fim de obter, adulterar ou destruir dados, informações ou documentos eletrônicos, sem autorização ou excedendo a autorização concedida, passa a ser punida com reclusão de 1 a 4 anos, além de multa. Essa pena é agravada quando o crime resulta em prejuízo econômico à vítima, chegando a uma reclusão de 2 a 5 anos, mais multa. (BRASIL, 2021)

É importante ressaltar que, além do agravamento das penas, a Lei 14.155/2021 também estabelece que os crimes cibernéticos passam a ser considerados como delitos de alta lesividade social, o que pode influenciar na concessão de benefícios penitenciários, como a progressão de regime, de forma mais restritiva. Isso reflete o entendimento de que os crimes digitais têm o potencial de causar danos significativos não apenas às vítimas, mas também à sociedade como um todo.

Esse agravamento das penas é visto por muitos como uma resposta necessária às mudanças no cenário dos crimes digitais. Conforme ressalta Barreto (2020), a tecnologia avançou a tal ponto que os crimes cibernéticos não são mais considerados simples infrações, mas sim ameaças sérias à segurança e à privacidade das pessoas. Portanto, é fundamental que a legislação esteja alinhada com essa realidade e possa desencorajar eficazmente a prática desses crimes.

A Lei 14.155/2021 também prevê o agravamento da pena para o crime de furto qualificado quando cometido por meio de fraude eletrônica, como o uso de dispositivos ou programas para subtrair informações ou valores. Além disso, a legislação estabelece que o estelionato cometido de forma eletrônica, com o intuito de obter vantagem ilícita, também será punido com pena maior do que o estelionato tradicional.

A proteção dos dados pessoais dos usuários e a segurança no ambiente digital são preocupações cada vez mais relevantes na sociedade moderna. Nesse sentido, a Lei 14.155/2021

representa um avanço significativo no sentido de dissuadir a prática de crimes digitais, garantindo que a legislação seja uma ferramenta eficaz no combate a esses delitos.

No entanto, é importante destacar que a eficácia da legislação não depende apenas do agravamento das penas, mas também da capacidade de investigação e punição por parte das autoridades competentes. Como observa Andrade (2019), o combate aos crimes cibernéticos envolve a necessidade de recursos técnicos e humanos especializados para rastrear e identificar os criminosos, o que representa um desafio adicional.

Desta feita, a Lei 14.155/2021 marca um avanço significativo na legislação brasileira no combate aos crimes digitais, agravando as penas para invasão de dispositivos, furto qualificado e estelionato cometidos no ambiente digital. Essa legislação reflete a importância de adaptar o ordenamento jurídico às mudanças tecnológicas e proteger a sociedade contra as ameaças que surgem no ambiente digital. No entanto, é fundamental que as medidas sejam acompanhadas por investimentos em recursos humanos e técnicos para garantir a eficácia na aplicação da lei.

2.6 A importância e a necessidade da constante evolução da legislação penal para repreensão dos crimes digitais

A necessidade de atualização constante da legislação penal para abordar os crimes digitais é evidente quando se observa a rapidez com que a tecnologia evolui. Como aponta Andrade (2019, p. 156), "a internet é um ambiente em constante mutação, com novas tecnologias e ferramentas surgindo constantemente". Essa dinâmica impõe desafios significativos às autoridades e legisladores, que devem acompanhar de perto essas mudanças para garantir que as leis permaneçam relevantes e eficazes.

Um dos principais motivos para a constante evolução da legislação penal no combate aos crimes digitais é a diversificação das ameaças. Os criminosos cibernéticos estão constantemente desenvolvendo novas táticas e técnicas para contornar as leis existentes e explorar novas vulnerabilidades. Como observa Barreto (2020, p. 183), "os hackers e os criminosos cibernéticos são notórios por sua capacidade de se adaptar rapidamente às mudanças tecnológicas e legais". Isso exige que a legislação seja flexível e ágil o suficiente para lidar com essas ameaças em constante evolução.

Além disso, a globalização da internet torna os crimes digitais uma preocupação transnacional. Os criminosos muitas vezes operam de jurisdições estrangeiras, tornando difícil a

aplicação das leis nacionais. Nesse contexto, a cooperação internacional é essencial, e as leis devem ser atualizadas para permitir a colaboração entre países na investigação e persecução desses crimes (LIMA, 2019).

Outro fator que destaca a necessidade de constante evolução da legislação penal é a crescente dependência da sociedade em relação à tecnologia e à internet. Com a digitalização de setores como saúde, finanças e infraestrutura crítica, os crimes cibernéticos podem ter sérias repercussões, afetando não apenas indivíduos, mas também organizações e até mesmo a segurança nacional (ANDRADE, 2019). Portanto, as leis devem ser adaptadas para proteger esses setores vitais da economia e da sociedade.

A evolução da legislação penal no campo dos crimes digitais não se limita apenas à criação de novos tipos penais. Também envolve a revisão e aprimoramento das leis existentes para refletir as realidades digitais. Isso inclui questões como a definição de jurisdição, a obtenção de evidências eletrônicas, a proteção da privacidade dos indivíduos e a punição proporcional aos infratores (ALMEIDA, 2018).

Um exemplo notável da necessidade de evolução legislativa é a Lei dos Crimes Cibernéticos dos Estados Unidos, conhecida como Lei CFAA (Computer Fraud and Abuse Act). Esta lei, que foi originalmente promulgada em 1986, passou por várias emendas ao longo dos anos para abordar questões emergentes, como a crescente ameaça de hacking e a proteção de sistemas de computadores críticos (REZENDE, 2019).

Além disso, a evolução da legislação penal no combate aos crimes digitais também deve levar em consideração princípios fundamentais, como a proporcionalidade e a proteção dos direitos humanos. Como argumenta Barreto (2020, p.184), "as leis que combatem os crimes digitais devem ser formuladas de maneira que não comprometam os direitos à privacidade e à liberdade de expressão". Portanto, é essencial encontrar um equilíbrio entre a repressão eficaz dos crimes e a proteção das liberdades individuais.

A importância da constante evolução da legislação penal no combate aos crimes digitais também é ressaltada pelo aumento das ameaças cibernéticas em todo o mundo. Nos últimos anos, assistimos a ataques cibernéticos de grande escala que afetaram governos, empresas e instituições críticas. Esses eventos demonstram a urgência de atualizar e fortalecer as leis e os mecanismos de aplicação da lei para enfrentar essas ameaças (ROCHA, 2018).

Portanto, a importância e a necessidade de constante evolução da legislação penal para a repressão dos crimes digitais são evidentes diante das mudanças rápidas no cenário tecnológico e das crescentes ameaças cibernéticas. A adaptação das leis existentes e a criação de novas disposições legais são essenciais para proteger a sociedade, garantir a segurança das transações online e preservar os direitos fundamentais dos indivíduos na era digital.

CONSIDERAÇÕES FINAIS

A evolução da legislação penal no combate aos crimes cibernéticos é um tema de suma importância na sociedade contemporânea, onde a crescente dependência da tecnologia e da internet se traduz em novos desafios e ameaças à segurança e à privacidade dos cidadãos. Ao longo deste artigo, explorou-se como a legislação penal vem se adaptando para enfrentar os delitos no âmbito virtual, acompanhando a rápida evolução da tecnologia e buscando proteger os direitos e interesses da sociedade.

A internet e a revolução digital trouxeram inúmeras oportunidades e benefícios para a sociedade, mas também abriram caminho para uma nova categoria de crimes, os crimes cibernéticos. Entre estes crimes inclui-se o estelionato virtual, que representa uma ameaça significativa para a segurança online e a privacidade dos indivíduos. A rápida evolução da tecnologia, juntamente com a globalização da internet, tornou essencial que a legislação penal acompanhe essas mudanças para garantir que a sociedade esteja protegida.

Um dos marcos mais importantes na evolução da legislação penal no Brasil em relação aos crimes cibernéticos foi a promulgação da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann. Esta lei trouxe consigo a tipificação de crimes cibernéticos e estabeleceu penas para condutas como invasão de dispositivos, divulgação não autorizada de informações e outros atos prejudiciais praticados no ambiente digital. O nome da lei faz referência ao famoso caso da atriz Carolina Dieckmann, cujas fotos pessoais foram roubadas e divulgadas na internet, ilustrando a vulnerabilidade dos indivíduos no ambiente virtual.

Além disso, o Marco Civil da Internet, Lei nº 12.965/2014, representou um passo significativo no sentido de estabelecer diretrizes para o uso da internet no Brasil e garantir a proteção dos direitos dos usuários, incluindo a proteção de dados pessoais. Esta legislação estabelece princípios fundamentais, como a neutralidade da rede, a preservação da privacidade

dos usuários e a proteção de dados pessoais, que são essenciais para a construção de um ambiente digital seguro e equitativo.

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, é outra legislação relevante que merece destaque. Inspirada em regulamentações europeias, como o Regulamento Geral de Proteção de Dados (GDPR), a LGPD estabelece regras detalhadas para o tratamento de dados pessoais no Brasil. Ela impõe obrigações rigorosas às empresas que coletam e processam dados pessoais e dá aos indivíduos maior controle sobre suas informações pessoais.

Recentemente, a Lei nº 14.155/2021 trouxe agravamento das penas para crimes de invasão de dispositivos, furto qualificado e estelionato ocorridos em meio digital, conectado ou não à internet. Esta lei reflete o reconhecimento de que os crimes cibernéticos estão se tornando cada vez mais sofisticados e prejudiciais, exigindo uma resposta legal mais robusta.

No entanto, a constante evolução da legislação penal no combate aos crimes cibernéticos não deve ser vista apenas como uma questão de imposição de penas mais severas. Ela também engloba aspectos como a proteção dos direitos individuais, a garantia da privacidade e o equilíbrio entre a repressão aos delitos e a preservação das liberdades civis. Assim, é fundamental que as leis que combatem os crimes digitais sejam formuladas de maneira a não comprometer esses direitos fundamentais à privacidade e à liberdade de expressão.

Outro ponto relevante a ser destacado é a necessidade de cooperação internacional no combate aos crimes cibernéticos. Dado que muitos criminosos operam de jurisdições estrangeiras, a coordenação entre países é essencial para investigar e perseguir esses delitos de forma eficaz. Nesse contexto, acordos e tratados internacionais desempenham um papel importante na promoção da cooperação e no enfrentamento conjunto das ameaças cibernéticas.

A evolução da legislação penal no combate aos crimes cibernéticos também deve considerar a educação e a conscientização pública. À medida que as pessoas se tornam mais conscientes das ameaças digitais, elas podem adotar práticas mais seguras online e contribuir para a prevenção de delitos. Além disso, a formação de especialistas em cibersegurança e a capacitação das forças de segurança são fundamentais para lidar com a complexidade desses crimes.

É importante ressaltar que, embora a legislação seja uma ferramenta fundamental no combate aos crimes cibernéticos, ela não é a única solução. A segurança cibernética envolve uma abordagem multidisciplinar que combina medidas legais, técnicas e educacionais. Empresas,

governo, organizações não governamentais e a sociedade como um todo desempenham um papel crucial na proteção contra ameaças digitais.

No entanto, à medida que a tecnologia continua a evoluir e novos desafios cibernéticos surgem, a adaptação da legislação penal permanece como um pilar central na defesa dos interesses da sociedade. A legislação deve ser flexível o suficiente para lidar com ameaças em constante mutação e equilibrar a proteção dos direitos individuais com a repressão dos delitos.

Portanto, com fulcro em tudo que fora exposto, a evolução da legislação penal no combate aos crimes cibernéticos é uma necessidade premente em um mundo cada vez mais digitalizado. As leis devem acompanhar a rápida evolução da tecnologia e da sociedade, garantindo a proteção dos direitos e interesses dos cidadãos. A promulgação de leis como a Lei Carolina Dieckmann, o Marco Civil da Internet, a LGPD e a Lei nº 14.155/2021 reflete o compromisso do Brasil em enfrentar os desafios da era digital. No entanto, o trabalho não está concluído, pois os crimes cibernéticos continuarão a evoluir, exigindo uma resposta legal igualmente adaptável e eficaz.

REFERÊNCIAS

ALMEIDA, Gabriela Pinheiro. **Crimes Cibernéticos: uma análise da legislação brasileira e perspectivas de prevenção.** Dissertação (Mestrado em Direito) - Universidade de Brasília, 2018.

ANDRADE, Nilo José Nascimento de. **A investigação de crimes cibernéticos no Brasil e os desafios para a efetivação do devido processo legal**. In Anais do 1º Congresso Internacional de Ciência, Tecnologia e Inovação., 2019.

BARRETO, A. SANTANA, M. **A evolução da legislação de crimes cibernéticos: desafios e perspectivas**. Revista de Direito e Tecnologia, 14(2), 37-56, 2018.

BARRETO, Jorge Henrique. **A vulnerabilidade dos sistemas de informação como fundamento para a criminalização dos delitos informáticos**. Revista Jurídica Cesumar, 20(1), 175-195, 2020.

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: 20/11/2023

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20/11/2023

CLARKE, R.; KNAKE, R. **Cyber War: The Next Threat to National Security and What to Do About It**. HarperCollins, 2010.

DONEDA, Danilo. **Da Proteção de Dados Pessoais à LGPD: Comentários à Lei nº 13.709/2018**. Editora Forense, 2019.

FONSECA, Andreia Barbosa. **Crimes Cibernéticos: Desafios e Perspectivas**. São Paulo: Editora Juruá, 2017.

HOLT, T. J.; BOSSLER, A. M. **Cybercrime in a Global Information Age**. Cambridge University Press, 2017.

KSHETRI, N. **International Perspectives on Cybercrime**. Routledge, 2017.

JUNGER, S.; RUESSELER, H. **Cybercrime and Cybersecurity in the Global South: Challenges and Perspectives.** Springer, 2017.

LIMA, Mariana Ribeiro. **Legislação e Crimes cibernéticos: A necessidade de adaptação**. In: Anais do Congresso Nacional de Direito Cibernético, 2019.

OLIVEIRA, André. **Investigação de Crimes Cibernéticos: Aspectos Práticos e Jurídicos**. São Paulo: Thomson Reuters Brasil, 2017

OLIVEIRA, Pedro Silva. **Lei Geral de Proteção de Dados: Impactos e desafios para a privacidade online**. Brasília: Editora ABC, 2020.

ORTELLADO, Pablo. **Internet, Mobilização e Política: A Comunicação Digital do Movimento Fora do Eixo.** Editora Elefante, 2019.

RABELO, M. S. R. **A cooperação internacional no combate aos crimes cibernéticos**. Revista de Direito Internacional, v. 17, n. 1, p. 56-77, 2020.

REDDY, V. et al. **Handbook of Research on Cyber Crime and Information Privacy**. IGI Global, 2018.

REZENDE, Amanda. **A importância da Lei Geral de Proteção de Dados para o cidadão brasileiro, 2019.** Disponível em: https://canaltech.com.br/seguranca/a-importancia-da-lei-geral-de-protecao-de-dados-para-o-cidadao-brasileiro-150596/. Acesso em: 20/11/2023

RIBEIRO, Carlos Alberto. **Legislação e Crimes Cibernéticos: O papel das leis na era digital**. São Paulo: Editora Jurídica, 2019.

ROCHA, João Paulo. **Crimes Cibernéticos e a Sensação de Impunidade**. Revista de Direito Digital, v. 12, n. 3, 2018.

SANTOS, Lucas. **Crimes Cibernéticos: Responsabilidade Civil e Proteção de Dados**. São Paulo: Editora Revista dos Tribunais, 2019

SANTOS, Luísa Maria. **Marco Civil da Internet: Direitos e Deveres dos Usuários**. São Paulo: Editora Digital, 2016.

SILVA, Ana Paula. **Crimes Cibernéticos e Sociedade Democrática**. Revista de Direito Digital, v. 15, n. 1, 2020.

SILVA, M. C. **Crimes cibernéticos: uma análise jurídica**. Revista de Direito, Tecnologia e Inovação, v. 4, n. 2, p. 107-128, 2020.

SILVEIRA, Sergio Amadeu da. **Marco Civil da Internet: A Carta de Princípios da Rede no Brasil**. Editora Boitempo, 2015.

SOUZA, Rafael Barbosa. **Lei 14.155/2021: Agravamento das Penas para Crimes Cibernéticos**. In: Anais do Congresso Nacional de Direito Cibernético, 2021.