Cognitio Juris
ISSN 2236-3009

CRIMES CIBERNÉTICOS NO BRASIL: DESAFIOS E A APLICABILIDADE DA LEGISLAÇÃO

CYBER CRIMES IN BRAZIL: CHALLENGES AND THE APPLICABILITY OF THE LEGISLATION

Artigo submetido em 24 de maio de 2023
Artigo aprovado em 02 de junho de 2023
Artigo publicado em 10 de junho de 2023

Cognitio Juris
Ano XIII – Número 47 – Junho de 2023
ISSN 2236-3009

.

Autor:
Jonas Milhomem Araújo[1]
Israel Andrade Alves [2]

.

RESUMO

O presente trabalho teve como objetivo analisar os desafios enfrentados pelo Brasil no combate aos crimes cibernéticos e a aplicabilidade da legislação vigente nesse contexto. Foram realizadas pesquisas bibliográficas e documentais para a coleta de informações e dados relevantes sobre o tema. Os resultados da pesquisa indicam que os crimes cibernéticos são um desafio crescente para o Brasil, sendo que a falta de investimentos em tecnologia e treinamento especializado são os principais obstáculos para o combate a esses

crimes. Além disso, a aplicabilidade da legislação existente é limitada, sendo necessária uma atualização para garantir a efetividade do combate aos crimes cibernéticos. Por fim, o estudo conclui que o combate aos crimes cibernéticos no Brasil ainda é um desafio complexo, que requer uma abordagem multidisciplinar e o envolvimento de diversos setores da sociedade. Além disso, é necessária uma atualização da legislação e a implementação de políticas públicas que visem fortalecer a capacidade do país para lidar com esses crimes.

Palavras-chave: Crimes cibernéticos; Legislação; Políticas públicas.

ABSTRACT

The present work aimed to analyze the challenges faced by Brazil in the fight against cyber crimes and the applicability of current legislation in this context. Bibliographical and documentary research was carried out to collect relevant information and data on the subject. The survey results indicate that cyber crimes are a growing challenge for Brazil, and the lack of investments in technology and specialized training are the main obstacles to combating these crimes. In addition, the applicability of existing legislation is limited, requiring an update to ensure the effectiveness of the fight against cybercrime. Finally, the study concludes that the fight against cybercrime in Brazil is still a complex challenge, which requires a multidisciplinary approach and the involvement of different sectors of society. Furthermore, it is necessary to update legislation and implement public policies aimed at strengthening the country's capacity to deal with these crimes.

Keywords: Cyber crimes; Legislation; Public policy.

INTRODUÇÃO

A crescente popularização da tecnologia da informação e a evolução da internet têm trazido inúmeros benefícios para a sociedade, possibilitando o acesso a informações e serviços de forma rápida e eficiente. No entanto, juntamente com essas vantagens, surgiram também os

crimes cibernéticos, que representam um grande desafio para as autoridades policiais e os especialistas em segurança da informação.

O Brasil não está imune a esse problema, e nos últimos anos, tem sido alvo de diversos tipos de crimes cibernéticos, tais como fraudes bancárias, roubo de informações pessoais e empresariais, invasão de sistemas e sabotagem virtual. Esses crimes causam prejuízos financeiros, danos à reputação das empresas e violação da privacidade das pessoas.

Para enfrentar esse cenário, o país possui uma legislação específica que prevê a punição para os crimes cibernéticos. No entanto, a aplicabilidade dessa legislação ainda é um desafio, devido à falta de investimentos em tecnologia e treinamento especializado, além da dificuldade de cooperação internacional para a investigação e repressão desses crimes.

Diante desse contexto, o presente trabalho tem como objetivo analisar os desafios enfrentados pelo Brasil no combate aos crimes cibernéticos e a aplicabilidade da legislação vigente nesse contexto. Serão realizadas pesquisas bibliográficas e documentais para a coleta de informações e dados relevantes sobre o tema. Com essa pesquisa, espera-se contribuir para o debate sobre a efetividade das medidas adotadas pelo governo brasileiro para combater os crimes cibernéticos, bem como para a conscientização da sociedade sobre os riscos da falta de segurança digital e a importância de políticas públicas que visem fortalecer a capacidade do país para lidar com esses crimes.

Assim, o presente estudo se justifica pela relevância do tema e pela necessidade de um olhar crítico sobre a situação atual do combate aos crimes cibernéticos no Brasil. Além disso, a pesquisa poderá contribuir para a identificação de soluções e estratégias que possam ser adotadas para mitigar os efeitos desses crimes na sociedade e na economia brasileira.

Dessa forma, este trabalho está organizado em 3 capítulos, além desta introdução. O primeiro capítulo apresenta uma revisão bibliográfica sobre os conceitos de crimes cibernéticos, das redes Sociais e Mídias, as principais ameaças e os avanços tecnológicos

para o aumento dos delitos. O segundo capítulo aborda sobre a lei brasileira e sua eficácia contra os crimes cibernéticos, bem como a aplicabilidade e combate dos crimes cibernéticos e os desafios enfrentados na investigação e nas punições.

Por fim, o terceiro capítulo trata da necessidade de avanços legislativos e a proteção das informações.

1. CRIMES CIBERNÉTICOS NO BRASIL

1.1 CRIMES CIBERNÉTICOS – DEFINIÇÕES

Crimes cibernéticos, também conhecidos como crimes eletrônicos ou crimes digitais, referem-se a ações criminosas que são praticadas utilizando tecnologias da informação e comunicação (TICs). Esses crimes podem ser definidos como "toda e qualquer conduta delitiva praticada com o auxílio de recursos da informática, que possa afetar a segurança e a integridade de sistemas, programas ou dados" (SILVA, 2018, p. 41).

Segundo Mattos (2018, p. 25), "os crimes cibernéticos podem ser praticados por indivíduos ou organizações, e visam desde o simples vandalismo até o roubo de informações confidenciais e o comprometimento da segurança nacional de um país". Dessa forma, os crimes cibernéticos abrangem uma ampla variedade de atividades criminosas, tais como invasão de sistemas, roubo de informações, sabotagem virtual, fraude bancária, pirataria de software, entre outras.

De acordo com Ferreira, os crimes cibernéticos podem ser classificados em quatro categorias principais:

Crimes contra a integridade, crimes contra a confidencialidade, crimes contra a disponibilidade e crimes contra a propriedade. Os crimes contra a integridade envolvem a modificação ou destruição de dados ou sistemas, como por exemplo, a disseminação de vírus ou o ataque a sites. Já os crimes contra a confidencialidade estão relacionados ao acesso ou

divulgação não autorizados de informações protegidas, como o roubo de senhas ou a interceptação de comunicações. Os crimes contra a disponibilidade referem-se à prática de ações que comprometem a disponibilidade de serviços ou recursos de TICs, como o ataque de negação de serviço (DDoS). E, por fim, os crimes contra a propriedade envolvem a utilização ilegal de propriedade intelectual, como a pirataria de software ou o download ilegal de filmes e músicas (FERREIRA, 2021, p. 16).

Para Capistrano e Silva (2019, p. 7), a evolução constante da tecnologia e o uso crescente da internet pela população tornam os crimes cibernéticos uma ameaça cada vez mais presente na sociedade atual. Além disso, esses autores destacam que a facilidade de anonimato na rede, a falta de regulação adequada e a falta de conscientização da população sobre segurança digital são fatores que contribuem para o aumento desses crimes.

Segundo Côrtes (2020, p. 4), a legislação brasileira define os crimes cibernéticos como delitos eletrônicos e prevê a punição para esses crimes em leis específicas, como a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que trata dos crimes cometidos contra a intimidade sexual na internet, e a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), que estabelece normas para a proteção de dados pessoais na internet.

Portanto, é importante ressaltar que os crimes cibernéticos representam um desafio para as autoridades policiais e os especialistas em segurança da informação, e que a prevenção e combate a esses crimes exigem uma abordagem multidisciplinar, envolvendo tanto medidas de segurança técnica quanto aprimoramento da legislação e das estratégias de investigação e repressão. Como destaca Luna (2019, p. 23), é necessário um trabalho conjunto entre setores públicos e privados, com a participação de profissionais de diversas áreas, como jurídica, tecnológica, policial e psicológica, para uma atuação efetiva contra os crimes cibernéticos.

Além disso, é fundamental que as empresas e usuários estejam conscientes sobre a

importância da segurança digital e adotem medidas preventivas para evitar serem vítimas desses crimes. Segundo Silva (2018, p. 43), algumas medidas simples podem ser adotadas, como o uso de antivírus atualizados, a criação de senhas seguras, a não compartilhamento de informações pessoais e a utilização de conexões seguras em redes públicas.

Sendo assim, é importante ressaltar que os crimes cibernéticos não são um problema exclusivo do Brasil, mas sim uma preocupação global. A Organização das Nações Unidas (ONU) tem se empenhado em discutir e desenvolver ações de combate aos crimes cibernéticos, através da elaboração de tratados internacionais e cooperação entre países (FERREIRA, 2021, p. 23).

Diante disso, é fundamental que o Brasil esteja preparado para enfrentar os desafios apresentados pelos crimes cibernéticos, através da adequação da legislação, da adoção de medidas de segurança e da conscientização da população sobre a importância da segurança digital. Somente dessa forma será possível garantir a proteção dos direitos fundamentais dos cidadãos e a segurança do ambiente virtual.

1.2 REDES SOCIAIS E MÍDIAS

As redes sociais e mídias são elementos fundamentais na sociedade contemporânea, desempenhando um papel importante na comunicação, informação e interação entre pessoas e organizações. De acordo com Boyd e Ellison (2008, p. 211), uma rede social é um serviço online que permite aos usuários construir um perfil público ou semi-público, conectando-se com outros usuários, compartilhando conteúdo e interagindo em comunidades virtuais.

As mídias, por sua vez, referem-se ao conjunto de plataformas de comunicação que permitem a disseminação de informações e conteúdos diversos, tais como textos, imagens, vídeos e áudios. As mídias são caracterizadas pela convergência, ou seja, pela integração de diferentes tecnologias e plataformas que permitem a criação e distribuição de conteúdo

pelos usuários (JENKINS, 2008, p. 21).

Entre as redes sociais mais populares atualmente estão o Facebook, Twitter, Instagram, LinkedIn, Snapchat e TikTok. Já entre as mídias, destacam-se a televisão, o rádio, os jornais e revistas, bem como as plataformas digitais como o YouTube, Netflix, Amazon Prime e Spotify. O surgimento das redes sociais e mídias trouxe consigo uma série de mudanças no modo como as pessoas se comunicam, interagem e consomem informações. De acordo com Castells (2008, p. 29), as redes sociais e mídias são elementos centrais na formação da sociedade em rede, caracterizada pela conectividade e interação em tempo real entre indivíduos e organizações.

No entanto, as redes sociais e mídias também apresentam desafios e riscos, como a disseminação de fake news, o cyberbullying e o uso inadequado de dados pessoais. Segundo Sibilia (2019, p. 38), as redes sociais e mídias criaram uma nova forma de sociabilidade, mas também trouxeram consigo novas formas de exclusão e controle social.

Diante dessas questões, é fundamental que os usuários estejam cientes dos riscos e desafios associados às redes sociais e mídias, adotando medidas preventivas para garantir sua segurança e privacidade online. Além disso, é importante que as autoridades e empresas estejam atentas à necessidade de regulamentação e monitoramento dessas plataformas, visando garantir a proteção dos direitos fundamentais e o combate aos crimes cibernéticos (FREITAS, 2020, p. 25).

Sendo assim, as redes sociais e mídias são elementos fundamentais na sociedade contemporânea, desempenhando um papel importante na comunicação, informação e interação entre pessoas e organizações. No entanto, também apresentam desafios e riscos que exigem uma abordagem cuidadosa e multidisciplinar, envolvendo medidas de segurança, regulação e conscientização dos usuários.

1.3 PRINCIPAIS AMEAÇAS

As redes sociais e mídias se tornaram um ambiente propício para o surgimento de uma série de ameaças que comprometem a segurança e privacidade dos usuários. Dentre as principais ameaças, podemos citar a disseminação de fake news, o cyberbullying, o phishing, o stalking, o vazamento de dados pessoais, a exposição indevida de informações sensíveis, entre outros (CASTRO, 2021, p. 25).

A disseminação de fake news é uma das principais ameaças das redes sociais e mídias. Trata-se da divulgação de informações falsas ou distorcidas, que podem causar prejuízos à reputação, imagem e segurança dos usuários. De acordo com Sibilia (2019, p. 54), as fake news se tornaram uma ameaça global, capaz de influenciar processos eleitorais, a saúde pública e a segurança nacional.

O cyberbullying é outra ameaça comum nas redes sociais e mídias, caracterizado pela prática de intimidação, humilhação, difamação e perseguição de indivíduos ou grupos online. Segundo Patchin e Hinduja (2018, p. 21), o cyberbullying pode ter consequências graves, como o desenvolvimento de transtornos mentais e o aumento do risco de suicídio.

O phishing é uma técnica de engenharia social que tem como objetivo obter informações pessoais e financeiras dos usuários, como senhas e dados bancários. De acordo com McAfee (2020), o phishing é uma das ameaças mais comuns nas redes sociais e mídias, sendo realizado por meio de mensagens fraudulentas, anúncios enganosos e links maliciosos.

O stalking, ou perseguição online, é uma ameaça que consiste na vigilância excessiva e invasão da privacidade de uma pessoa, por meio do monitoramento de suas atividades nas redes sociais e mídias. Conforme aponta Cassidy e Sutherland (2019, p. 14), o stalking pode levar ao desenvolvimento de transtornos psicológicos e físicos, bem como ao risco de violência e assédio sexual.

O vazamento de dados pessoais é uma ameaça que envolve a exposição indevida de informações sensíveis dos usuários, como dados de identificação, histórico de navegação,

informações financeiras e médicas, entre outros. De acordo com Kaspersky (2021), os vazamentos de dados pessoais têm se tornado cada vez mais frequentes nas redes sociais e mídias, comprometendo a privacidade e segurança dos usuários.

A exposição indevida de informações sensíveis é outra ameaça comum nas redes sociais e mídias, envolvendo a divulgação de informações íntimas ou privadas dos usuários, como fotos, vídeos e conversas pessoais. Segundo Sibilia (2019, p. 62), a exposição indevida pode levar à violação dos direitos fundamentais, bem como à criação de situações de constrangimento e humilhação.

Além dessas ameaças, as redes sociais e mídias também são alvo de ataques cibernéticos, como invasões de contas, roubo de senhas e infecções por malware. Conforme aponta Kaspersky (2021), os ataques cibernéticos nas redes sociais e mídias podem ter como objetivo a obtenção de informações confidenciais dos usuários, como dados bancários, informações pessoais e senhas, ou até mesmo a propagação de vírus e malware para comprometer o dispositivo do usuário.

Outra ameaça comum nas redes sociais e mídias, de acordo com Safernet Brasil:

É a propagação de conteúdo impróprio ou ilegal, como imagens de violência, pornografia infantil, discurso de ódio e incitação à violência. A disseminação desses conteúdos pode ter impactos graves na sociedade, como o aumento da violência e do crime organizado (SAFERNET, 2021, p. 15).

Por fim, é importante mencionar a possibilidade de manipulação de informações e opiniões nas redes sociais e mídias, por meio de técnicas como a criação de perfis falsos, o uso de bots e a compra de curtidas e seguidores. Segundo alude Tufekci (2017, p. 19), a manipulação da opinião pública nas redes sociais e mídias tem se tornado uma ameaça à democracia, comprometendo a transparência e a veracidade das informações.

Diante dessas ameaças, é fundamental que os usuários das redes sociais e mídias estejam atentos e adotem medidas para proteger sua privacidade e segurança online. Além disso, é necessário que as empresas responsáveis por essas plataformas implementem medidas eficazes para prevenir e combater as ameaças cibernéticas e garantir a integridade e segurança de seus usuários.

1.4 AVANÇOS TECNOLÓGICOS PARA O AUMENTO DOS DELITOS

Ocorre que os avanços tecnológicos têm trazido inúmeras facilidades e benefícios para a sociedade, mas também têm sido um dos principais fatores que contribuem para o aumento dos delitos cibernéticos. Como aponta Citron (2019), a tecnologia tem permitido que os criminosos atuem de forma mais sofisticada e eficiente, com a utilização de técnicas avançadas de invasão, engenharia social e criptografia.

Sendo assim, um dos principais avanços tecnológicos que têm sido explorados pelos criminosos é o uso da inteligência artificial (IA). De acordo com o autor McAfee (2021), a IA pode ser utilizada para automatizar e otimizar os processos de invasão, identificação de vulnerabilidades e até mesmo para a criação de malware personalizado. Outra tecnologia que tem sido bastante utilizada pelos criminosos é o blockchain, que foi criado para trazer mais segurança e transparência às transações financeiras. No entanto, conforme destaca Jansen e Lopes (2019), o blockchain também pode ser utilizado para a realização de transações ilícitas, como o comércio de drogas e armas, por meio de criptomoedas.

Além do mais, a popularização da Internet das Coisas (IoT) tem trazido novas vulnerabilidades e desafios para a segurança cibernética. Conforme aponta Kim (2018), a interconexão entre dispositivos inteligentes pode permitir que os criminosos acessem informações pessoais e sensíveis dos usuários, como dados de saúde e informações bancárias.

Outro avanço tecnológico que também tem sido usado pelos criminosos é o deepfake, que

consiste na criação de vídeos e imagens falsas utilizando técnicas de inteligência artificial. De acordo com Edwards:

O deepfake pode ser utilizado para a disseminação de desinformação e para a realização de ataques de phishing. Apopularização do acesso à internet em dispositivos móveis, o que tem permitido que os criminosos realizem ataques a qualquer hora e em qualquer lugar (EDWARDS, 2022, p. 18-20).

Em conformidade com Norton (2021), a utilização de smartphones e tablets para acessar a internet e realizar transações financeiras tem trazido novos desafios para a segurança cibernética, como a necessidade de proteger as informações pessoais dos usuários em dispositivos móveis.

Diante desses avanços tecnológicos, é fundamental que as autoridades e empresas responsáveis pela segurança cibernética estejam sempre atualizadas e preparadas para enfrentar as ameaças cibernéticas cada vez mais sofisticadas e complexas.

2. A LEI BRASILEIRA E SUA EFICÁCIA CONTRA OS CRIMES CIBERNÉTICOS

2.1 DA APLICABILIDADE E COMBATE DOS CRIMES CIBERNÉTICOS

A classificação dos crimes cibernéticos pode ser dividida em três categorias, nomeadamente crimes puros que visam a violação de sistemas informáticos por hackers, crimes mistos que exploram a internet para cometer crimes como transferências ilegais de bens ou valores e crimes comuns como pornografia infantil que utiliza a internet como ferramenta para a realização de atividades ilícitas, o que já é reconhecido pela lei e enfatizado no Estatuto da Criança e do Adolescente.

A segunda classificação de crimes inclui aqueles que são cometidos exclusivamente por meio de computadores, bem como crimes impróprios que lesam o público em geral, sendo os ambientes virtuais apenas uma das formas de execução do crime, que também pode ser

feito por outros métodos.

Conforme pesquisa de Barreto publicada em 2017, a incidência de crimes cibernéticos está em constante crescimento, deixando os usuários expostos e indefesos contra possíveis ataques. Além disso, a legislação brasileira relativa ao crime cibernético é inadequada e não abrange toda a gama de crimes cibernéticos existentes, nem fornece limites legais apropriados ou definições para esses crimes (BARRETO, 2017).

A maioria dos crimes cibernéticos impróprios é penalizada de acordo com o desatualizado Código Penal de 1940. Em muitos casos, o princípio da analogia é utilizado como o único método eficaz para garantir que os cibercriminosos não consigam escapar das repercussões legais. No entanto, em Direito Penal, o princípio da tributação é violado por esta abordagem, uma vez que exige o desenvolvimento de leis mais particulares. Como resultado, é inadequado confiar no princípio da analogia para ações legais em tais casos (BARRETO, 2017).

São normas aplicadas, com a uso da analogia, aos crimes virtuais, exemplos:

Calúnia (art. 138 do Código Penal); Difamação (art. 139 do Código Penal); Injúria (art. 140 do Código Penal); Ameaça (art. 147 do Código Penal); Furto (art. 155 do Código Penal); Dano (art. 163 do Código Penal); Apropriação indébita (art. 168 do Código Penal); Estelionato (art. 171 do Código Penal); Violação ao direito autoral (art. 184 do Código Penal); Pedofilia (art. 240 e 241 da Lei nº 8.069/90 – Estatuto da Criança e do Adolescente); art. 234 (Pornografia Infantil); Crime contra a propriedade industrial (art. 183 e ss. da Lei nº 9.279/96); Interceptação de comunicações de informática (art. 10 da Lei nº 9.296/96); Interceptação de E-mail Comercial ou Pessoal (art. 10 da Lei nº 9.296/96); Crimes contra software – "Pirataria" (art. 12 da Lei nº 9.609/98) (SANTANA, 2021, p. 15).

Em sua publicação de 2020, Medeiros e Ugalde (2020), especialistas na área de criminologia, fornecem um resumo abrangente dos crimes cibernéticos mais frequentes. Os artigos 138,

139 e 140 do Código Penal apresentam disposições legais para crimes contra a honra, que se aplicam tanto à atividade criminosa virtual quanto à não virtual. O artigo 234 do Código Penal trata da pornografia infantil, que abrange atividades como importação, exportação, aquisição ou posse de objetos obscenos com a intenção de distribuí-los ou exibi-los comercialmente ou publicamente, incluindo escrever, desenhar, pintar e imprimir. A pena para esses delitos é de detenção de seis meses a dois anos ou multa.

O ato de pornografia infantil é amplamente reconhecido como forma de violência sexual contra crianças e adolescentes, sendo considerado crime pelo Estatuto da Criança e do Adolescente (ECA) por meio da lei federal 8.069/1990, alterada pela lei 11.829/2008. A tipificação da pedofilia como crime pode ser encontrada nos artigos 240 e 241 da Lei 8.069/1990 (ECA), que estabelecem as disposições necessárias:

“Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:

Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

§ 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.

“Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.”

Já o artigo 171, do CP: “obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa. E os crimes contra a propriedade intelectual que lesam expressamente o direito autoral, encontra respaldo no

artigo 184: Violar direitos de autor e os que lhe são conexos: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa. (BRASIL, 1990, s/p).

Conforme a referência de Barreto (2017), sugere-se que a Lei nº 7.232/84 foi uma das primeiras leis que se concentraram nos crimes cibernéticos e estabeleceu princípios e diretrizes pertinentes à Política Nacional de Informática (PNI) por meio da criação do Conselho Nacional de Informática (CONIN). Como resultado, a legislação adicional foi implementada para proteger os bens jurídicos e as relações no mundo virtual. A Lei nº 7.646/87 foi tornada obsoleta pela Lei nº 9.609/98, que dispunha sobre a comercialização e propriedade intelectual de programas de computador no Brasil. Essa lei também reconheceu como crime a violação de tais bens (BARRETO, 2017):

Art. 35. Violar direitos de autor de programas de computador: Pena – Detenção, de 6 (seis) meses a 2 (dois) anos e multa.

Art. 37. Importar, expor, manter em depósito, para fins de comercialização, programas de computador de origem externa não cadastrados:

Pena – Detenção, de 1 (um) a 4 (quatro) anos e multa (BRASIL, 1998, s/p).

A Convenção de Budapeste, instituída em 2001 pelo Conselho da Europa na Hungria, tem como foco os crimes mundiais no âmbito digital, priorizando a implementação de políticas de combate aos crimes cibernéticos e proteção da sociedade por meio de legislação específica e apoio internacional. Apesar disso, o Brasil não aderiu à convenção. Adicionalmente, a implementação da Lei 12.735, de 30 de novembro de 2012, pode ser considerada um avanço significativo, pois foi alterada para trazer mudanças no atual marco legal, conforme abaixo:

Art. 1º: Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico,

digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências (BRASIL, 2012, s/p).

Sendo assim, a Lei Federal n° 12.737/2012 foi acrescentada para tratar da questão dos crimes cibernéticos, amplamente condenados pela sociedade, mas muitas vezes impunes por falta de fiscalização legal.

A lei em questão trata da tipificação dos crimes cibernéticos, e faz alterações ao Decreto-Lei nº 2.848 do CP. É comumente chamada de "Lei Carolina Dieckmann" devido ao fato de que durante sua passagem pela Câmara dos Deputados, a atriz foi vítima de crime virtual quando suas fotos privadas vazaram sem sua permissão (RODRIGUES, 2020).

Segundo Almeida (2015), a lei em questão nasceu do Projeto de Lei nº 2.793/2011, apresentado por Paulo Teixeira (PT-SP) durante sua gestão como Deputado em 2011. O projeto teve tramitação urgente no Congresso Nacional, ao contrário outros projetos semelhantes abordando crimes de computador. Ao introduzir os artigos 154-A e 154-B e alterar os existentes artigos 266 e 298, o CP foi alterado pela lei:

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e 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. (Incluído pela Lei nº 12.737, de 2012) (BRASIL, 2011,

s/p).

Conforme argumentam Matsuyama e Lima (2017), o Brasil tem dado passos largos no âmbito da realidade virtual. Isso foi possível por meio da implementação da Lei nº 12.965/2014, também conhecida como Marco Civil da Internet. A lei traça vários princípios, responsabilidades e garantias para a utilização da internet no Brasil. Os referidos estudiosos garantiram a inovação ao priorizar a liberdade de expressão e a privacidade dos usuários, com foco específico na neutralidade da rede – o tratamento justo e igualitário do acesso à internet, sem qualquer forma de discriminação, limitação, bloqueio ou cobrança diferenciada dos serviços de internet existentes.

Segundo constatado por Ribeiro (2020), os provedores de internet são obrigados por lei a salvaguardar os registros de suas atividades e usuários durante o uso de suas plataformas e serviços. Isso é para garantir a segurança dos indivíduos, tanto legal quanto fisicamente, que utilizam o meio digital, pondo fim à noção de “terra sem lei”.

É fundamental destacar o incidente ocorrido em 2015 que envolveu o WhatsApp como protagonista. Devido às suas políticas de proteção em relação aos dados do usuário, o serviço tornou-se objeto de escrutínio legal que exigia a exposição da comunicação de seus usuários para auxiliar nas investigações criminais. A empresa responsável pela aplicação recusou-se a fornecer as informações solicitadas, levando o tribunal a decidir suspender o serviço em todo o país. (RIBEIRO, 2020).

A Lei 14.155/21, uma recente adição ao marco legal, introduziu medidas mais rigorosas para penalizar o furto e furto digital, especialmente aqueles cometidos em computadores, celulares e tablets. Essa nova lei também altera a lei n. 2.828 do CP, ampliando a punição para crimes como pirataria de aparelhos, furto qualificado e apropriação cometida no meio digital, independentemente de haver ou não conexão com a internet (GANEM, 2017).

A pena por furto é de prisão de quatro a oito anos. A punição pela invasão de dispositivo de

computador, prevista no artigo 154-A do CP, foi recentemente agravada. O período de detenção aumentou de três meses para um ano, e a prisão agora é de um para quatro anos. Além disso, se o hacker resultar em prejuízo financeiro, a pena é aumentada de um terço a dois terços. No caso de peculato, a pena de detenção é de quatro a oito anos, acrescida de multa, quando a vítima for enganada e fornecer seus dados pessoais por meio de redes sociais. Além disso, se o crime for cometido contra pessoa idosa ou vulnerável ou se for utilizado servidor fora do país, a pena por peculato é aumentada.

O objetivo das leis descritas e explicadas neste tópico foi revisar e modernizar a legislação que dificultou a categorização de crimes cibernéticos. Seu objetivo era defender os princípios que fundamentam o Direito Penal, como a proibição da analogia e da legalidade, e priorizar a proteção dos usuários. No entanto, essas leis são inadequadas diante da lacuna regulatória e da impunidade que persiste na luta contra os crimes cibernéticos. Como tal, há uma necessidade urgente de um quadro legal mais específico e eficiente.

2.2 DESAFIOS ENFRENTADOS NA INVESTIGAÇÃO E NAS PUNIÇÕES

Os crimes cibernéticos representam um desafio para as autoridades policiais e para o sistema jurídico, já que muitos deles acontecem em âmbito global, dificultando a identificação dos responsáveis e a aplicação das leis. De acordo como destaca Figueiredo (2019), a falta de cooperação entre os países e a falta de uniformidade nas legislações são alguns dos principais desafios para a investigação e punição dos crimes cibernéticos.

Um dos principais desafios enfrentados pelas autoridades policiais é a falta de capacitação e recursos para lidar com as complexidades dos crimes cibernéticos. Segundo Garcia (2019), muitos profissionais da área de segurança pública não estão preparados para lidar com as tecnologias e técnicas utilizadas pelos criminosos cibernéticos, o que dificulta a identificação e prevenção desses crimes.

Para mais, a natureza anônima e virtual dos crimes cibernéticos dificulta a identificação dos

responsáveis. Como destaca Ribeiro (2019), muitos criminosos utilizam técnicas de anonimato, como a utilização de redes de computadores distribuídas (botnets), o que dificulta a identificação de sua localização e identidade.

Outro desafio enfrentado pelas autoridades é a falta de cooperação entre os países na investigação e punição dos crimes cibernéticos. A medida que descreve o autor Schneier (2021), muitos países não possuem legislações adequadas para lidar com os crimes cibernéticos ou não possuem acordos de cooperação para a troca de informações entre as autoridades policiais de diferentes países. Ademais, a dificuldade na coleta e preservação de evidências eletrônicas é outro desafio para a investigação e punição dos crimes cibernéticos. De acordo com Silva (2020), a falta de uma legislação específica que oriente a coleta e preservação de evidências eletrônicas pode comprometer a validade e admissibilidade dessas evidências em um processo jurídico.

A dificuldade em identificar os responsáveis por ataques cibernéticos de grande escala, como os ataques a infraestruturas críticas. Conforme aponta Marcos Weiss diz que:

Muitas vezes esses ataques são realizados por grupos organizados, que utilizam técnicas avançadas de criptografia e anonimato para dificultar a identificação dos responsáveis. Ocorre que a falta de uma legislação específica para os crimes cibernéticos também é um desafio para a aplicação da justiça (WEISS, 2019, p. 213).

Segundo Arantes (2019), a legislação brasileira não prevê todas as modalidades de crimes cibernéticos e nem estabelece penas proporcionais à gravidade desses crimes. A necessidade de acompanhar constantemente as evoluções tecnológicas e as técnicas utilizadas pelos criminosos cibernéticos é outro desafio enfrentado pelas autoridades. Para Souza (2021), as técnicas de invasão e engenharia social estão em constante evolução, o que exige que as autoridades policiais estejam sempre atualizadas para lidar com as novas ameaças cibernéticas.

É importante ressaltar que a falta de cooperação internacional também é um grande desafio para a investigação e punição de crimes cibernéticos. Como esses crimes podem ser cometidos a partir de qualquer lugar do mundo, muitas vezes é difícil para as autoridades de um país identificarem e prenderem um suspeito que está em outro país. De acordo com o Relatório da ONU sobre cibercrime (2020), a falta de cooperação internacional tem sido um obstáculo significativo para a aplicação da lei no combate aos crimes cibernéticos. Os governos precisam trabalhar juntos para desenvolver acordos de cooperação e compartilhamento de informações que permitam a investigação e a punição dos criminosos cibernéticos em todo o mundo.

A investigação e punição de crimes cibernéticos é uma das principais dificuldades atualmente, tendo em vista que a natureza complexa desses crimes. Muitos crimes cibernéticos envolvem redes complexas de criminosos que se escondem atrás de várias camadas de anonimato e criptografia. Identificar e rastrear esses criminosos pode ser um processo demorado e difícil. Ocorre que, a maioria dos crimes cibernéticos envolve transações financeiras complexas, o que dificulta ainda mais a identificação dos perpetradores. De acordo com Prenzler (2013), a complexidade desses crimes significa que as autoridades policiais precisam ter um alto nível de especialização e treinamento para investigar e punir com sucesso os criminosos cibernéticos.

A falta de conscientização e de conhecimento por parte do público em geral sobre os crimes cibernéticos. Muitas pessoas não sabem como se proteger contra esses crimes ou o que fazer se se tornarem vítimas. Isso pode tornar mais difícil para as autoridades policiais identificar e investigar esses crimes. Segundo os autores Holt e Bossler (2017), a educação do público sobre os crimes cibernéticos é crucial para ajudar a reduzir o número de vítimas e aumentar as chances de identificar e punir os criminosos.

Bem como a falta de recursos financeiros e tecnológicos disponíveis para as autoridades policiais. Muitas vezes, os departamentos de polícia não têm acesso aos recursos necessários

para lidar com crimes cibernéticos, como a tecnologia de ponta e os especialistas em segurança da informação. Isso pode dificultar a investigação e a punição desses crimes. Para o autor Caballero (2015), as autoridades policiais precisam de investimentos significativos em tecnologia e treinamento para acompanhar a evolução dos crimes cibernéticos.

Segundo Kshetri alude que:

Outra empecilho enfrentado é a falta de padronização das leis e regulamentos em todo o mundo pode criar obstáculos na investigação e punição de crimes cibernéticos. As leis e regulamentos variam significativamente de um país para outro, o que pode dificultar a cooperação internacional e a extradição de criminosos de um país para outro. Portanto, a falta de padronização das leis e regulamentos é uma barreira significativa para o combate aos crimes cibernéticos em todo o mundo (KSHETRI, 2018, p. 95).

Ocorre que a rapidez com que os criminosos cibernéticos podem adaptar suas técnicas e táticas. Como a tecnologia está novas vulnerabilidades e criar novas formas de ataques, dificultando o trabalho dos investigadores e das autoridades policiais. Segundo Reynolds (2019), a falta de atualização constante da legislação é outro obstáculo que dificulta a investigação e punição desses crimes. A legislação precisa ser atualizada com frequência para acompanhar as mudanças no cenário cibernético e garantir que as autoridades policiais tenham as ferramentas necessárias para combater esses crimes.

Sendo assim, o caráter transnacional dos crimes cibernéticos também é um desafio para a investigação e punição desses delitos. Os criminosos cibernéticos podem operar em qualquer lugar do mundo, o que dificulta a identificação e captura dos suspeitos. Muitas vezes, eles utilizam servidores em países com leis mais brandas ou sem cooperação internacional, o que dificulta ainda mais a investigação e a cooperação entre as autoridades policiais de diferentes países (BASKIN, 2019).

Desta forma, as autoridades enfrentam também é a falta de colaboração por parte das

vítimas de crimes cibernéticos. Muitas vezes, as vítimas não relatam o crime por medo de retaliação ou constrangimento. Além disso, em alguns casos, as vítimas não percebem que foram alvo de um crime cibernético, o que dificulta a investigação e a punição dos responsáveis (DUGGAL, 2021). Bem como:

A falta de recursos técnicos e financeiros também é um desafio para a investigação e punição dos crimes cibernéticos. As autoridades policiais muitas vezes não possuem recursos suficientes para realizar investigações avançadas e contratar especialistas em segurança da informação para auxiliá-los na investigação desses delitos. Isso dificulta a identificação dos criminosos e a coleta de provas, o que pode resultar em impunidade (BASKIN, 2019, p. 4092).

Ocorre que a falta de padronização na coleta de evidências em crimes cibernéticos. Diferentes países e jurisdições têm abordagens diferentes para a coleta de evidências e a aplicação da lei em casos de crimes cibernéticos. Isso pode levar a inconsistências nos processos de investigação e punição desses crimes (DUGGAL, 2021).

Ocorre que a privacidade dos usuários da Internet é um assunto delicado, e as autoridades precisam equilibrar a necessidade de coletar evidências para investigar crimes cibernéticos com a necessidade de proteger a privacidade dos indivíduos. Isso pode levar a conflitos e desafios legais que dificultam a investigação e punição desses delitos (REYNOLDS, 2019).

Portanto, que o combate aos crimes cibernéticos é um trabalho em conjunto, no qual a conscientização e educação do público em geral sobre os riscos e perigos da Internet é necessário, pois acabe se tornando outro desafio no qual dificulta a prevenção e combate aos crimes cibernéticos. Muitas pessoas ainda não entendem os riscos associados ao uso da Internet e não tomam medidas adequadas para proteger suas informações pessoais e privacidade online. Portanto, teve haver políticas públicas e conscientização e prevenção.

3. DA NECESSIDADE DE AVANÇOS LEGISLATIVOS

A crescente incidência de crimes cibernéticos tem destacado a necessidade de avanços legislativos no Brasil e em todo o mundo. A complexidade e a evolução rápida das tecnologias digitais e a globalização das atividades criminosas impõem um desafio constante às autoridades em termos de legislação adequada para combater tais crimes.

Como destaca Amaral (2019), o Brasil ainda carece de uma legislação específica para crimes cibernéticos, o que dificulta a investigação e a punição dos responsáveis por esses delitos. A legislação atualmente em vigor é insuficiente para lidar com as novas formas de criminalidade na era digital.

Segundo Souza (2017), a legislação brasileira precisa acompanhar os avanços tecnológicos para garantir a proteção dos direitos dos cidadãos e a segurança das informações na era digital. A lei precisa ser mais clara em relação à tipificação dos crimes cibernéticos e às penalidades correspondentes. Ademais, é importante que a legislação brasileira preveja a cooperação internacional entre as autoridades responsáveis pela investigação e punição de crimes cibernéticos. Para Stela (2019), os crimes cibernéticos muitas vezes têm dimensão transnacional, o que torna essencial a cooperação internacional para a sua investigação e punição.

Também é necessário que haja uma maior conscientização sobre a importância da segurança cibernética e dos riscos associados aos crimes cibernéticos. Como ressalta Figueiredo (2018), a legislação por si só não é suficiente para prevenir e combater os crimes cibernéticos. É necessário que haja uma conscientização da população sobre a segurança digital e a adoção de medidas de prevenção.

Ademais, é importante que a legislação preveja a responsabilização das empresas provedoras de serviços digitais por crimes cibernéticos cometidos por seus usuários. Para Mendes (2019), muitos crimes cibernéticos são cometidos por meio de plataformas e redes sociais, e as empresas provedoras desses serviços devem ser responsabilizadas por não

adotarem medidas adequadas para prevenir tais crimes.

Ocorre que a legislação também deve prever a proteção dos dados pessoais dos usuários e a responsabilização das empresas que não garantam a segurança desses dados. De acordo com Barros (2020), a proteção dos dados pessoais é essencial para a privacidade e segurança dos indivíduos na era digital, e as empresas devem ser responsabilizadas por eventuais vazamentos ou uso indevido desses dados. Sendo assim, é relevante mencionar que a legislação preveja a capacitação adequada das autoridades responsáveis pela investigação e punição de crimes cibernéticos. Pois para Nunes (2021), a capacitação e atualização constante dos profissionais envolvidos na investigação de crimes cibernéticos são essenciais para garantir a efetividade das investigações e punições.

Diante do exposto, é necessário que a legislação brasileira avance para acompanhar os avanços tecnológicos e garantir a proteção dos cidadãos na era digital. A atualização das leis e a conscientização da população sobre a importância da segurança cibernética são essenciais para reduzir os crimes cibernéticos no país.

De acordo com Barros e Marques (2021), a Lei Carolina Dieckmann, de 2012, que tipifica os crimes cibernéticos, foi um passo importante na legislação brasileira, mas ainda existem lacunas a serem preenchidas. Alguns especialistas argumentam que a lei não é suficientemente ampla e atualizada para abordar todas as possíveis formas de crimes cibernéticos. Outrossim, a lei não trata de questões como a coleta e armazenamento de dados pessoais, que se tornaram cada vez mais importantes com o crescente uso da internet.

Sendo assim, um aspecto a ser considerado é a cooperação internacional para o combate aos crimes cibernéticos. Segundo Oliveira (2019), a cooperação entre países é fundamental para investigar e processar os autores de crimes cibernéticos que atuam em diferentes jurisdições. É necessário, portanto, que o Brasil participe de acordos e tratados internacionais

que abordem a questão da segurança cibernética.

As empresas e provedores de serviços on-line também devem ser responsabilizados por seus papéis na prevenção e combate aos crimes cibernéticos. Como destacado por Serrano (2021), as empresas têm a responsabilidade de implementar medidas de segurança robustas para proteger os dados pessoais dos usuários e colaborar com as autoridades em caso de incidentes de segurança.

Desta forma, é necessário que a legislação seja clara e adequada à realidade atual, mas também flexível o suficiente para se adaptar às mudanças tecnológicas e às novas ameaças à segurança cibernética. Para Lopes (2019), a legislação precisa ser atualizada constantemente para se manter relevante e eficaz na prevenção e punição dos crimes cibernéticos. Portanto, é preciso que o poder legislativo, o judiciário, as empresas e a sociedade como um todo trabalhem em conjunto para desenvolver uma legislação atualizada e eficaz que possa proteger os cidadãos na era digital.

3.1 DA PROTEÇÃO DAS INFORMAÇÕES

No que tange a proteção das informações é um aspecto fundamental da segurança cibernética. Em conformidade com os autores Garcia e Meira (2019), a segurança das informações é um elemento-chave para garantir a privacidade, a integridade e a confidencialidade dos dados pessoais dos usuários. Nesse sentido, é necessário que sejam implementadas medidas de segurança adequadas para proteger essas informações.

Uma das medidas mais importantes é a criptografia, que consiste em codificar as informações de modo que apenas o destinatário possa acessá-las. Segundo Rezende (2021), a criptografia é um importante mecanismo de segurança para proteger as informações contra possíveis ataques e ameaças cibernéticas. Dessa forma, é possível garantir a privacidade das informações dos usuários e prevenir possíveis violações.

Além de que é indispensável que as empresas e os usuários adotem práticas seguras de armazenamento e gerenciamento de informações. De acordo com Carvalho e Fonseca (2021), a adoção de medidas de segurança como senhas fortes, autenticação de dois fatores e backups regulares são essenciais para proteger as informações contra possíveis violações e garantir a recuperação das informações em caso de perda ou roubo.

Outra medida que pode ser de grande relevância é a conscientização dos usuários sobre a importância da proteção de informações e os riscos associados à exposição desnecessária de informações pessoais. Segundo Siqueira (2021), a educação do usuário é uma medida importante para a prevenção de possíveis violações de informações e a conscientização dos riscos relacionados à exposição desnecessária de informações pessoais.

Sendo assim, as empresas implementem políticas de privacidade claras e transparentes para informar aos usuários sobre como as informações são coletadas, armazenadas e utilizadas. Segundo Barros e Marques (2021), as políticas de privacidade são uma importante medida de proteção das informações dos usuários e devem ser implementadas de forma clara e acessível. Em síntese, é importante que sejam implementadas medidas de segurança para proteger as informações contra possíveis ataques e ameaças cibernéticas. Em harmonia com Oliveira (2019), a implementação de medidas de segurança adequadas, como firewalls, antivírus e sistemas de detecção de intrusão, são essenciais para proteger as informações contra possíveis violações e ataques cibernéticos.

Em virtude disso, a proteção das informações é um elemento-chave da segurança cibernética. É necessário que sejam implementadas medidas de segurança adequadas, além da conscientização dos usuários e a adoção de práticas seguras de armazenamento e gerenciamento de informações.

CONCLUSÃO

Diante do exposto, conclui-se que os crimes cibernéticos representam uma ameaça

significativa para a segurança digital e a privacidade das pessoas no Brasil e em todo o mundo. Esses crimes envolvem diversas práticas ilícitas, como roubo de informações, invasão de sistemas, phishing, ransomware, entre outros. Tais práticas são realizadas por meio da internet e de outras tecnologias digitais, o que torna ainda mais difícil a identificação e punição dos criminosos.

Os desafios para a investigação e punição dos crimes cibernéticos são muitos, incluindo a falta de treinamento e recursos adequados por parte das autoridades policiais, a complexidade técnica e a velocidade com que os criminosos podem adaptar suas técnicas. Além disso, a legislação brasileira ainda é insuficiente para lidar com esses crimes de maneira efetiva, o que torna ainda mais difícil a proteção dos cidadãos.

É fundamental que sejam tomadas medidas para enfrentar esses desafios e combater os crimes cibernéticos de forma mais efetiva. Isso inclui a necessidade de treinamento e investimento em tecnologias de segurança da informação por parte das autoridades policiais, bem como a atualização da legislação para incluir novas formas de crimes cibernéticos e aumentar as penalidades para esses delitos.

Além disso, é importante que as empresas e indivíduos adotem medidas de proteção de informações, como a utilização de softwares antivírus, senhas fortes e criptografia, para reduzir as chances de serem vítimas de crimes cibernéticos. A conscientização sobre as práticas seguras na internet também é fundamental para evitar a exposição de dados pessoais e financeiros a criminosos. É fundamental que haja uma colaboração estreita entre governos, empresas e sociedade civil para enfrentar a ameaça dos crimes cibernéticos e proteger as pessoas na era digital. Essa colaboração deve incluir a troca de informações e melhores práticas, o investimento em tecnologias de segurança da informação e a promoção de uma cultura de segurança digital.

Sendo assim, os crimes cibernéticos representam um desafio significativo para a segurança

digital e a privacidade das pessoas no Brasil e em todo o mundo. A proteção contra esses crimes exige uma abordagem colaborativa e multidisciplinar, que inclua a adoção de medidas de proteção de informações, a atualização da legislação e o investimento em tecnologias de segurança da informação por parte das autoridades policiais e empresas.

REFERÊNCIAS

ARANTES, T. (2019). **Crimes cibernéticos: desafios jurídicos e políticas públicas no Brasil. Revista Brasileira de Políticas Públicas**, 9(2), 185-200.

AMARAL, Luiz Augusto. **A criminalidade cibernética no Brasil: entre a insegurança jurídica e a necessidade de tutela penal efetiva**. In: OLIVEIRA, Maria de Fátima; FREITAS, Gabriel; CUNHA, Rodrigo (Orgs.). Direito, comunicação e tecnologia: desafios e perspectivas. São Paulo: Editora Atlas, 2019. p. 141-160.

BASKIN, Alison S.; DOSSETT, Lesly A.; HARRIS, Chelsea A. **Cultural complications curriculum: applicability to surgical oncology programs and practices.** Annals of Surgical Oncology, v. 28, n. 8, p. 4088-4092, 2019.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências.** Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 12 mai. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet); e dá outras providências. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 mai.

2023.

BRASIL. **Lei 12.735 de 30 de novembro de 2012**. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 12 mai. 2023.

BOYD, Danah M.; ELLISON, Nicole B. **Social network sites: definition, history, and scholarship. Journal of Computer-Mediated Communication**, v. 13, n. 1, p. 210-230, 2008.

BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei n. 12.737/2012**, março 2017. Disponível em: http://www.conteudojuridico.com.br/consulta/artigos/49678/crimes-ciberneticos-sob- a-egide-da-lei-12-737-2012. Acesso em: 10/05/2023.

BARROS, M. C. S., & Marques, F. M. C. (2021). **A problemática da segurança cibernética: análise do arcabouço legal brasileiro.** Revista de Direito, Tecnologia e Inovação, 8(1), 97-116.

CARVALHO, A. M. B., & Fonseca, B. M. (2021). **Cibercrime: principais ameaças e medidas de prevenção.** Revista Científica Internacional, 3(2), 56-68.

CAPISTRANO, Marcos; SILVA, Raimundo Nonato Macedo da. **Crimes cibernéticos: Uma análise da evolução tecnológica e da legislação brasileira.** Revista Novas Tecnologias na Educação, v. 17, n. 1, p. 1-10, 2019.

CASTELLS, Manuel. **A sociedade em rede**. 9. ed. São Paulo: Paz e Terra, 2008.

CASTRO, L. C. (2021). **Os perigos da internet: riscos, ameaças e desafios na era digital**. São Paulo: Novatec Editora.

CASSIDY, C. M., & Sutherland, I. (2019). **Stalking and Harassment on Social Media.** In Social Media and Mental Health (pp. 13-24). Academic Press.

CABALLERO, J. (2015). **Policing cybercrime: Networked and social media technologies for predicting, preventing, and detecting digital crime**. Routledge.

CITRON, D. K. (2019). **Cyber Civil Rights**. Cambridge: Harvard University Press.

CÔRTES, Marcos E. O. **Crimes cibernéticos: legislação e investigação**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

EDWARDS, John. **Applying Signal Processing to Opposite Sides of Imaging: Separate European research projects are focusing on aspects of completely real and entirely fake images** [Special Reports]. IEEE Signal Processing Magazine, v. 39, n. 5, p. 18-20, 2022.

FERREIRA, Mário. **Crimes cibernéticos: prevenção e investigação.** São Paulo: Editora Brasport, 2021.

FREITAS, Rafaela Lopes de. **Redes sociais e mídias: proteção dos direitos fundamentais e combate aos crimes cibernéticos**. Revista da Faculdade de Direito de Ribeirão Preto, v. 4, n. 2, p. 277-294, 2020.

FERREIRA, Isabella. **Crimes cibernéticos: aspectos penais e processuais penais**. 2. ed. São Paulo: Editora Saraiva Educação, 2021.

FIGUEIREDO, C. (2019). **Crimes cibernéticos: investigação, prevenção e cooperação internacional.** Revista de Direito Digital e Compliance, 1(1), 117-129.

GANEM, G. B. **O impacto da lei de crimes digitais no Brasil**. Revista de Direito, Tecnologia e Inovação, v. 3, n. 2, p. 86-98, 2017.

GARCIA, L. P. (2019). **Desafios enfrentados pelas forças de segurança na investigação**

de crimes cibernéticos. Monografia de Conclusão de Curso, Curso de Direito, Universidade Estadual de Maringá.

Holt, T. J., & Bossler, A. M. (2017). **Cybercrime awareness and online victimization: Analyzing the role of gender and crime-fear. Journal of Interpersonal Violence**, 32(3), 365-385. doi: 10.1177/0886260515618286

JENKINS, Henry. **Convergence culture: where old and new media collide**. New York: New York University Press, 2008.

KSHETRI, N. (2018). **Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management**, 39, 80-89. doi: 10.1016/j.ijinfomgt.2017.12.005.

KSHETRI, Nir; VOAS, Jeffrey. **Blockchain-enabled e-voting.** Ieee Software, v. 35, n. 4, p. 95-99, 2018

KASPERSKY. (2021). **O que é um vazamento de dados e como ele pode afetar você**. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-a-data-breach. Acesso em: 12 maio 2023.

KIM, H. (2018). **Internet of Things security and privacy issues and solutions.** In 2018 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 1068-1070). IEEE.

Lei nº 11.829, de 25 de novembro de 2008. **Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para estabelecer o direito à convivência familiar e comunitária de crianças e adolescentes em regime de acolhimento institucion**al. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso em: 12 mai.

2023.

Lei nº 12.735, de 30 de novembro de 2012. **Altera a Lei no 9.472, de 16 de julho de 1997, quanto à prestação do serviço de acesso à internet e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 12 maio 2023.

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: 12 mai. 2023.

LUNA, Fabrício Martins. **Cibercrime e cyberbullying: aspectos penais e processuais penais**. 2. ed. São Paulo: Editora Atlas, 2019.

MATSUYAMA, Keniche Guimarães; LIMA, JAA. **Crimes cibernéticos: atipicidade dos delitos**. 2017. Disponível em:< joaoademar.qlix.com.br/3cbpj.pdf>. Acesso em: 20 nov 2019.

MATTOS, Fabrício da Mota. **Crimes cibernéticos: prevenção, investigação e repressão**. 2. ed. rev., atual. e ampl. São Paulo: Atlas, 2018.

MEDEIROS, Gutembergue Silva; UGALDE, Júlio César Rodrigues. **Crimes Cibernéticos: Considerações Sobre a Criminalidade na Internet**, setembro 2020. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/crimes- ciberneticos-consideracoes-sobre-a-criminalidade-na-internet/. Acesso em: 12/05/2022.

MENDES, Caio César Vieira. **Responsabilidade das empresas provedoras de serviços de internet pelos crimes cibernéticos cometidos por meio de suas plataformas**. Revista Jus Navigandi, Teresina, ano 24, n. 5768, 22 abr. 2019. Disponível em: https://jus.com.br/artigos/73181/responsabilidade-das-empresas-provedoras-de-servicos-de-i

nternet-pelos-crimes-ciberneticos-cometidos-por-meio-de-suas-plataformas. Acesso em: 12 mai. 2023.

MCAFEE. (2020). **Phishing**. https://www.mcafee.com/blogs/consumer/phishing/

NORTON. (2021). **Mobile Security Threats: Protect Your Smartphone or Tablet**. https://us.norton.com/internetsecurity-mobile-mobile-security-threats-protect-your-smartphone-or-tablet.html

PATCHIN, J. W., & Hinduja, S. (2018). **Cyberbullying: An Update and Synthesis of the Research.** In R. Arnett (Ed.), The Oxford Research Encyclopedia of Communication. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228613.013.642

PRENZLER, T. (2013). **Policing cybercrimes: Situating the public police in networks of security governance.** Policing and Society, 23(3), 266-285.

STELA, F. (2019). **A importância da cooperação internacional para combater os crimes cibernéticos.** Revista Brasileira de Inteligência, Segurança e Defesa, (4), 44-60.

SANTANA, Roque Felipe da Silva et al. **Crimes cibernéticos: análise evolutiva da legislação penal brasileira e seus desafios**. 2021.

SAFERNET Brasil. (2021). **Denúncia Online.** Retrieved from https://new.safernet.org.br/denuncie.

SIBILIA, Paula. **Redes ou paredes: a escola em tempos de dispersão**. São Paulo: Cosac Naify, 2019.

SILVA, Raimundo Nonato Macedo da. **Crimes cibernéticos: Uma análise crítica da legislação brasileira**. Revista Direito, Estado e Sociedade, v. 53, p. 249-265, 2018.

SILVA, Marcelo Xavier da. **Crimes eletrônicos e segurança da informação.** 4. ed. São

Paulo: Editora Atlas, 2018.

RODRIGUES, Mariane; LIMA, Inayá Farias de; FREITAS, Rafael de. **Crimes cibernéticos à luz dos crimes contra a honra**. ANAIS CONGREGA MIC-ISBN: 978- 65-86471-05-2 e ANAIS MIC JR.-ISBN: 978-65-86471-06-9, v. 16, p. 354-359, 2020.

TUFEKCI, Z. (2017). **Twitter and Tear Gas: The Power and Fragility of Networked Protest**. Yale University Press. WEISS, Marcos Cesar. Sociedade sensoriada: a sociedade da transformação digital. **Estudos avançados**, v. 33, p. 203-214, 2019.

---

[1] Graduando em Direito pela Faculdade Serra do Carmo – FASEC. Email: jonas97milhomem@gmail.com

[2] Mestrando em Prestação Jurisdicional e Direitos Humanos pela Universidade Federal do Tocantins e Escola Superior da Magistratura Tocantinense. Pós-graduado em Direito Público pela Pontifícia Universidade Católica de Minas Gerais. Professor de Direito Penal, Processo Penal e Prática Criminal no curso de Direito na Faculdade Serra do Carmo – FASEC. Delegado de Polícia Civil do Estado do Tocantins. Email: prof.israelalves@fasec.edu.br