UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

LAURO RAIMUNDO DE LUNA FILHO

A RELAÇÃO ENTRE CRIMINALIDADE E AS TECNOLOGIAS EMERGENTES DE INFORMAÇÃO E COMUNICAÇÃO: TIC´S

JUAZEIRO DO NORTE-CE
2023

LAURO RAIMUNDO DE LUNA FILHO

A RELAÇÃO ENTRE CRIMINALIDADE E AS TECNOLOGIAS EMERGENTES DE INFORMAÇÃO E COMUNICAÇÃO: TIC´S

Trabalho de Conclusão de Curso – *Artigo Científico,* apresentado à Coordenação do Curso de Graduação em Direito do Centro Universitário Doutor Leão Sampaio, em cumprimento às exigências para a obtenção do grau de Bacharel.

Orientador: Prof. Esp. Francisco Gledison Lima Araújo.

JUAZEIRO DO NORTE-CE
2023

LAURO RAIMUNDO DE LUNA FILHO

TIC´S: A RELAÇÃO ENTRE CRIMINALIDADE E AS TECNOLOGIAS EMERGENTES DE INFORMAÇÃO E COMUNICAÇÃO

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de LAURO RAIMUNDO DE LUNA FILHO.

Data da Apresentação: 13/12/2023

BANCA EXAMINADORA

Orientador: PROF. ESP. FRANCISCO GLEDISON LIMA ARAÚJO/ UNILEÃO

Membro: PROF. ME. FRANCISCO THIAGO DA SILVA MENDES/ UNILEÃO

Membro: PROF. ME. OTTO RODRIGO CRUZ/ UNILEÃO

JUAZEIRO DO NORTE-CE
2023

TIC´S: A RELAÇÃO ENTRE CRIMINALIDADE E AS TECNOLOGIAS EMERGENTES DE INFORMAÇÃO E COMUNICAÇÃO

Lauro Raimundo de Luna Filho[1]
Prof. Esp. Francisco Gledison Lima Araújo[2]

RESUMO

Com a evolução da humanidade surgiu diversos avanços nas mais variadas áreas da sociedade e os meios digitais foi um das quais mais evolui. O nascimento da tecnologia e a era da informação aumentaram muito a vulnerabilidade do usuário, o que faz surgiu diversos mecanismos e orientações para inibir tais ações criminosas, principalmente os que são praticados de forma anônima e de difícil alcance dos acusados. No Brasil, os ataques cibernéticos estão cada vez mais desenvolvidos e complexos. Para erradicar esse problema e proteger os usuários que podem vir a ser vítimas desses crimes, foram elaboradas leis que inicialmente se mostraram promissoras, mas ao longo do tempo se mostraram ineficazes no combate a esses crimes, pelo fato da alta inovação da área. Assim, este estudo tem como objetivo se falta de regulamentação e controle adequados das TIC's pode contribuir para o aumento da criminalidade. Este trabalho é relevante pela necessidade de informar as pessoas sobre os graves riscos a que estão expostas diariamente devido às suas formas descuidadas de influência na Internet, e como agir em situações em que terceiros as expõem indevidamente ao ambiente virtual.

Palavras-chave: Crimes Cibernéticos. Tipicidade. Princípio da Legalidade. Inovação tecnológica.

ABSTRACT

With the evolution of humanity, there have been several advances in the most varied areas of society and digital media has been one of the ones that evolves the most. The birth of technology and the information age have increased the vulnerability of the user, which has led to the emergence of several mechanisms and guidelines to inhibit such criminal actions, especially those that are practiced anonymously and difficult to reach by the accused. In Brazil, cyberattacks are increasingly developed and complex. To eradicate this problem and protect users who may become victims of these crimes, laws were drafted that initially showed promise, but over time proved to be ineffective in combating these crimes, due to the high innovation in the area. Thus, this study aims to see if the lack of adequate regulation and control of ICTs can contribute to the increase in crime. This work is relevant due to the need to inform people about the serious risks to which they are exposed daily due to their careless forms of influence on the Internet, and how to act in situations where third parties unduly expose them to the virtual environment.

Keywords: Cyber Crimes. Typicality. Principle of Legality. Technological innovation.

[1]Graduando do Curso de Direito do Centro Universitário Doutor Leão Sampaio/Unileão. E-mail: Laurodaepp@gmail.com
[2] Professor Orientador. Email: gldaraujo@gmail.com

1 INTRODUÇÃO

A criminalidade é um problema que afeta diretamente a sociedade, causando prejuízos materiais e emocionais para as vítimas e a comunidade em geral. Com o avanço das tecnologias da informação e comunicação (TIC's), novas formas de criminalidade têm surgido, desafiando as instituições e autoridades responsáveis pela segurança pública.

A criminalidade sempre foi um desafio para a sociedade, causando prejuízos materiais e emocionais para as vítimas e a comunidade em geral. Com o avanço das tecnologias da informação e comunicação (TIC's), novas formas de criminalidade têm surgido, apresentando desafios adicionais para as autoridades responsáveis pela segurança pública.

O uso das TIC's tem transformado a maneira como as pessoas se relacionam, trabalham e se comunicam, proporcionando maior conectividade e facilidade de acesso à informação.

No entanto, essas mesmas tecnologias também têm sido utilizadas para fins ilegais, como o cibercrime, a disseminação de conteúdo ilícito pela internet, a invasão de sistemas, entre outros. Essas atividades criminosas apresentam novos desafios para as autoridades responsáveis pela segurança pública, que precisam desenvolver novas estratégias e tecnologias para combatê-las.

Dentre os diversos crimes, a invasão de sistemas é uma forma de criminalidade que vem aumentando cada dia mais, influenciando na segurança pública nacional, principalmente das empresas e indivíduos. Esse tipo de crime pode ser utilizado para obter informações confidenciais, roubar dinheiro, espionar atividades ou danificar sistemas. Além disso, a utilização de técnicas cada vez mais sofisticadas para a realização desses crimes.

Dessa forma, é necessário investigar as implicações dessas tecnologias na criminalidade e no combate à criminalidade, com o objetivo de desenvolver estratégias e tecnologias mais eficazes para lidar com esses desafios. Diante deste contexto surge a seguinte problemática: A falta de regulamentação e controle adequados das TIC's pode contribuir para o aumento da criminalidade?

Assim o objetivo geral para o presente estudo é analisar o impacto das novas tecnologias da informação e comunicação na criminalidade e como objetivos específicos: a) Identificar as principais formas de criminalidade que surgem com o avanço das TIC's; b) Analisar as estratégias utilizadas pelas autoridades responsáveis pela segurança pública para combater a criminalidade na era digital; c) Avaliar o papel da tecnologia na prevenção e investigação de crimes.

A importância do tema em questão para a sociedade está diretamente relacionada ao fato

de que as TIC's têm se tornado cada vez mais presentes no cotidiano das pessoas e das instituições, transformando a forma como as pessoas se comunicam, trabalham e interagem.

Dessa forma, é fundamental compreender as implicações das TIC na criminalidade e no combate à criminalidade, a fim de desenvolver estratégias e tecnologias mais eficazes para lidar com esses desafios.

Além disso, a falta de regulamentação e controle adequados das TIC pode contribuir para o aumento da criminalidade, já que a utilização de tecnologias sem o devido controle e fiscalização pode facilitar a realização de atividades criminosas. Nesse sentido, é fundamental que as instituições responsáveis pela segurança pública trabalhem em conjunto com as empresas de tecnologia e a sociedade civil para desenvolver políticas públicas específicas para a segurança digital, bem como para regulamentar e controlar o uso das TIC.

A metodologia adotada neste estudo foi predominantemente a revisão bibliográfica, com análise de textos legais, doutrina especializada, artigos científicos e demais materiais pertinentes ao tema. Esta abordagem permitiu uma análise aprofundada das questões jurídicas envolvidas na presente temática.

2 CRIMES CIBERNÉTICOS

De acordo com Nóbrega (2021), a concepção da internet remonta à década de 1940, quando foi desenvolvida com o propósito de ser uma ferramenta de comunicação militar durante a Guerra Fria, como uma alternativa caso os meios de comunicação convencionais falhassem.

Após o término da guerra, a internet passou a ser utilizada para fins sociais e marcou o surgimento de uma nova era, impulsionando o desenvolvimento do ENIAC, o primeiro computador digital, utilizado para cálculos balísticos (DOS SANTOS; MARTINS; TYBUCSH, 2017).

A internet, possibilitou uma infinidade de coisas, principalmente relacionada a facilidades do dia a dia e mesmo no mundo dos negócios. Porém, também possui o seu lado ruim, principalmente relacionado ao fato de que a internet, tem sido um instrumento utilizado para a prática de crimes. E justamente por ser um instrumento muito acessível, pode ser praticado por qualquer pessoa.

A pornografia da vingança, é uma dessas modalidades de crimes que tem se difundido por meio da internet, e basicamente se refere a divulgação de material de cunho íntimo, dentro da internet, com o intuito de provocar a outra parte, algum tipo de dano.

Nesse sentido, segundo Padovez e do Prado:

> O conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade (PADOVEZ; DO PRADO, 2019 p. 08).

Nesse sentido, segundo Lara (2021) a internet, apesar de ser um requisito indispensável ao funcionamento da sociedade, a legislação não tem conseguido ser eficiente o suficiente, para coibir todas as possíveis formas de violação que ela permite que sejam realizadas, e a quantidade de crimes como o pornô da vingança, é uma prova disso.

Nesse sentido, segundo Silva:

> Os crimes tradicionais relacionados à informática, descritos na legislação penal em vigor, mereceriam ser definidos em lei especial, para melhor interpretação e adequação. Com os recursos que a informática pode oferecer, a conduta delituosa chega quase que a perfeição dificultando, em muito, a sua identificação (SILVA, 2000 p.04).

Na esfera criminal, os mais comuns são os crimes virtuais que ofendem direta ou indiretamente a honra de alguém. Esses crimes, que são chamados de crimes contra a honra, têm previsão legal clara no Código Penal.

A simples distribuição de fotografias ofensivas ou insultos a alguém, ainda que a vítima seja desconhecida do autor, pode constituir um dos crimes contra a honra previstos nos artigos 138.º, 139.º e 140.º do Código Penal (CP), que são a difamação, a calúnia e a injúria, respectivamente (BRASIL, 1940).

O crime de difamação é estabelecido pelo artigo 138.º do CPC e consiste na mentira de que a vítima teria cometido um crime que não existiu ou não ocorreu, mas que a pessoa não é responsável e não está envolvida no mesmo. Entre os crimes contra a honra, o mais grave é a difamação, que prevê pena de prisão de seis meses a dois anos (CRESPO, 2015).

O crime de calúnia, cujo conceito está contido no artigo 139 do CP, é atribuir a alguém fato que ofenda sua reputação, que pode ser verdadeiro ou falso, de forma digno de respeito na vida pública, não uma maldição que leva a injúria. Nesse caso, a honra objetiva da vítima é alcançada, o que gera desconfiança por parte de terceiros ou da sociedade. Além disso, muitos autores conhecidos argumentam que as vítimas de difamação podem ser empresas e outras pessoas jurídicas (CRESPO, 2015).

Por fim, o crime de injúria, definido pelo artigo 140 do CP, está relacionado à violação da dignidade ou decência, xingamento ou atribuição de qualidades negativas, ou seja, quando

uma pessoa insulta, insulta, fala mal de outra. minar o conceito de vítima, afetando assim a autoestima. As lesões podem ser infligidas oralmente, por escrito, ou mesmo fisicamente, o que tem uma pena maior e se caracteriza quando os meios utilizados são considerados degradantes. O juiz também não pode impor uma sentença se a vítima tiver causado dano direto ou se a vítima responder imediatamente (CRESPO, 2015).

Além disso, se o insulto for causado por raça, cor, etnia, religião, procedência ou estado de velhice ou deficiência, o crime é denominado "dano discriminatório" (artigo 140, § 3º do Código Penal).

Os crimes acima não são admitidos na forma culposa, portanto, na prática, alguém que atenta a honra de outro não pode alegar que não sabia o que estava fazendo, uma vez que o dolo é um elemento subjetivo do tipo penal.

Todavia, é válido destacar que nos casos em que a vítima é funcionário público ofendido pelas suas funções, deve ser instaurado processo criminal pelo Ministério Público através da representação da vítima.

Estelionato digital: para enganar as vítimas, os criminosos usam sua vulnerabilidade para explorar suas emoções. Isso geralmente começa com a criação de uma página falsa que finge ser uma empresa que oferece oportunidades surreais à vítima em troca de uma certa quantia. Os golpistas simplesmente desaparecem após receber o valor, na maioria das vezes sem deixar rastros. O crime de fraude digital está previsto no artigo 171.º do Código Penal, que prevê pena de um a cinco anos de prisão e multa (GALINDO, 2022).

Alguns exemplos de desvios praticados pelos meios digitais: empréstimos com juros baixos ou simplesmente sem juros; oferecer um local com a inclusão da taxa da vítima e, na maioria das vezes, a pirâmide financeira, na qual, pagando a taxa de ingresso no esquema, o usuário deve convidar outras pessoas para participar do sistema (GALINDO, 2022).

Crime de ameaça: previsto no artigo 147 do Código Penal, que consiste em ameaçar alguém com palavras, gestos ou outros meios de lhe causar dano injusto e grave. A pena para esse crime, além de multa, pode variar de um a seis meses de prisão (BRASIL, 1940).

Crime de identidade falsa: previsto no artigo 307 do Código Penal. Este crime consiste em utilizar as redes sociais alheias ou mesmo fictícias em benefício próprio ou alheio ou praticar atos ilícitos, para os quais, além do pagamento de multa adicional, há pena de prisão de três meses a um ano (REIS, 2021).

Violações de segurança (senhas, bloqueios, sistemas de criptografia etc.): intrusão em um computador, rede, telefone celular ou dispositivo similar sem permissão para obter, falsifi-

car ou destruir dados ou informações, ou ainda instalar vírus ou vulnerabilidades em o dispositivo, previsto no artigo 154-A do Código Penal, que, além de pagar multa, prevê pena de reclusão de três meses a um ano (BRASIL, 1940).

Divulgação de materiais confidenciais: É a divulgação do conteúdo de um documento particular ou correspondência confidencial de terceiros sem justa causa, cuja divulgação pode prejudicar terceiros. O crime previsto no artigo 153.º do Código Penal é punível com pena de prisão de um a seis meses ou multa (JESUS; MILAGRE, 2016).

Comportamento obsceno: é um ato de insulto a terceiros em um local público aberto a terceiros ou aberto a terceiros. Este crime está previsto no artigo 233.º do Código Penal, que prevê pena de prisão de três meses a um ano ou multa.

Apologia ao crime: Qualquer pessoa que ofereça, transmita, venda, publique ou distribua registros de crimes violentos ou conteúdo que incentive sua prática. Nos casos em que o pedido de desculpas é feito online, a multa é dobrada. A infracção prevista no artigo 287.º é punível com pena de prisão de três a seis meses ou multa (SILVA, 2019).

Estupro virtual: De acordo com o disposto na Lei 12.015/09, que alterou o artigo 213 do Código Penal, o estupro virtual, para o qual não houve punição até o momento, tornou-se típico, o que aumentou muito a continuidade do seu programa. A prática desse crime ocorre quando a vítima é obrigada a criar conteúdo sexual sob ameaça de publicação de fotos e vídeos. Este crime é punível com pena de prisão de seis a dez anos (SILVA, 2019).

Vale lembrar que existem muitos outros crimes, ainda mais graves do que os citados acima, além do racismo, crimes de ódio, pornografia infantil, violações da liberdade religiosa, crimes virtuais contra a mulher e atos homofóbicos cometidos por esses indivíduos. que utilizam a Internet como uma ferramenta mais acessível e fácil para cometer esses crimes.

O primeiro passo é reunir provas do crime, bem como uma lista de testemunhas, o endereço de e-mail do site onde o crime foi cometido e a coleta e armazenamento de todos os materiais possíveis que possam servir de prova em tribunal, além de screenshots, WhatsApp, fotos, comentários, tweets, áudio, vídeo, URLs e e-mails. Portanto, mesmo que os perpetradores apreendam essas provas, as provas já foram coletadas adequadamente.

2.1 PROTEÇÃO QUANTO AOS CRIMES DIGITAIS

A segurança pública é uma forma de proteger e garantir os direitos humanos individuais, garantindo o pleno exercício da cidadania. De acordo com essa lógica, estando profundamente ligada à qualidade de vida dos cidadãos, a segurança pública é uma condição extremamente

importante para a efetivação da liberdade humana. Diante desse aspecto, ações preventivas e repressivas por parte do Estado tornam-se indispensáveis, principalmente no que diz respeito a atos criminosos. No entanto, nota-se que a segurança pública, de acordo com a constituição brasileira, também é responsabilidade de todos (SANTOS; MARTINS; TYBUCSH, 2018).

Atualmente, é perceptível o crescimento exponencial de todos os tipos de crimes que violam os direitos dos cidadãos e a segurança pública, dentre os quais está o objeto de estudo deste trabalho – o crime virtual.

Com o advento da Internet e o desenvolvimento das tecnologias de informação e comunicação, esse tipo de crime passou a ser amplamente utilizado por criminosos que, aproveitando-se da baixa cobertura e das oportunidades proporcionadas por esses sistemas de comunicação, cometem toda sorte de atos ilícitos (JULIANI, 2017).

A facilidade de interação na mídia, a capacidade de realizar operações bancárias, consultar qualquer informação e trocar mensagens com o mundo, atraíram as ações de criminosos que viam na Internet infinitas oportunidades de fraudes e roubos de informações por diversos meios fraudulentos para a prática do crime no mundo virtual (TOMÉ, 2018).

O crime virtual, segundo Otsu é definido

> Por conduta típica e ilícita que constitua crime ou contravenção, dolosa ou culposa, cometida ou dolosamente praticada por uma pessoa física ou pessoa jurídica que utilize tecnologia da informação dentro ou fora do ambiente de rede, e que viole direta ou indiretamente a segurança informática, cujos elementos são integridade, acessibilidade e confidencialidade (OTSU, 2023 p. 16).

Por possuírem características de atuação diferentes do crime geral, há a necessidade de uma abordagem diferente para obtenção de provas para esclarecê-lo. Essa diferenciação ocorre por meio de um cenário de crime parcial ou totalmente virtual. Nesta fase, há a necessidade de um exame especial que analise as evidências no ambiente computacional para orientar decisões importantes para a aplicação das sanções cabíveis.

Assim, o exame pericial computacional, segundo Batista (2017, p. 31), "[...] é uma ciência que utiliza métodos e habilidades especiais lida com a coleta, armazenamento e análise de dados eletrônicos durante um incidente de computador ou o uso de tecnologia de computador como meio para esse fim". Assim, ter a capacidade de envolver a polícia no trabalho investigativo para solucionar crimes cometidos com o auxílio de um computador.

No entanto, deve-se notar que existem métodos para proteger e prevenir o cibercrime. E é nesta fase que se torna importante considerar os aspectos relacionados com a segurança da informação, uma vez que esta é uma área específica do universo tecnológico, que revela os

conceitos e métodos de tratamento da informação relacionada com a segurança, sempre que dados ou informação inseridos.

Com esses aspectos em mente, Daniel (2022) defende que a informação é algo muito valioso que precisa ser protegido, e que certas políticas relacionadas à segurança devem ser tratadas com extrema cautela para evitar ameaças, principalmente, nos sistemas de comunicação.

As formas de proteção da informação devem ser inseridas no cotidiano dos usuários de qualquer sistema computacional de comunicação e processamento de dados, pois o sistema pode estar exposto a diversos tipos de ameaças que sem a devida proteção causam danos, muitas vezes irreparáveis, às informações (DA SILVA, 2023).

Muitos tipos de vírus e ataques estão se espalhando pela Internet para prejudicar pessoas, sistemas ou organizações e beneficiar criminosos. Recursos fundamentais que garantem a confidencialidade, integridade e disponibilidade das informações são fundamentais para a manutenção da segurança dos dados e da informação e aqueles que valorizam a integridade e relevância de seus dados e informações devem estar atentos a esses fundamentos.

Diante dessa perspectiva, buscam-se formas de minimizar a atividade criminosa relacionada ao mundo virtual aplicando conhecimentos e técnicas em diversos campos, encontrando subsídios que ofereçam garantias para a aplicação de sanções em todas as áreas. Isso requer investigação oportuna e séria, sempre levando em consideração o suporte das tecnologias disponíveis.

2.2 LEGISLAÇÃO BRASILEIRA: LEI CAROLINA DIECKMANN E A TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS

A Lei nº 12.737/2012, oficialmente conhecida como "Lei Carolina Dieckmann", representa um marco na legislação brasileira sobre crimes cibernéticos. O apelido da lei decorre de um caso de grande repercussão, em que a atriz brasileira Carolina Dieckmann teve fotos íntimas roubadas de seu computador pessoal e divulgadas na internet (ALVES. 2017).

Esta lei alterou o Código Penal Brasileiro para incluir explicitamente crimes cometidos no ambiente digital. A Lei define e pune a invasão de dispositivos informáticos, modificando o artigo 154-A do Código Penal para incluir a invasão de "dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou

tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" (Brasil, 2012).

A importância da Lei Carolina Dieckmann é ressaltada por Pereira e Ribeiro (2016, p. 108), que argumentam que a lei foi um passo significativo para a proteção de indivíduos contra violações de privacidade e outros crimes cibernéticos. A tipificação dos crimes cibernéticos trouxe maior segurança jurídica, tornando explícito que atividades prejudiciais no ciberespaço são reconhecidas e punidas.

Apesar do progresso representado da supracitada legislação, algumas críticas foram levantadas. Pinheiro (2021, p. 72) aponta que a lei pode não ser suficiente para combater a crescente sofisticação e diversidade dos crimes cibernéticos. A lei concentra-se principalmente na invasão de dispositivos, deixando lacunas em relação a outras formas de crimes cibernéticos.

A legislação em comento também se destaca como uma resposta à necessidade crescente de leis que tratem especificamente da proteção de dados pessoais e da privacidade na era digital. Conforme apontado por Boher (2019), a lei reflete um esforço em adaptar a legislação brasileira à realidade dos crimes informáticos e representa uma resposta direta aos desafios colocados pelas novas tecnologias.

Essa lei tem um papel particularmente importante na proteção dos cidadãos contra a violação de sua privacidade, a inclusão de crimes cibernéticos no Código Penal contribui para a proteção da privacidade e da intimidade, direitos fundamentais protegidos pela Constituição Brasileira.

No entanto, a aplicação da Lei nº 12.737/2012 não está isenta de desafios. Silva e Cavalcanti (2016) apontam que a implementação eficaz dessa lei requer não apenas a compreensão dos aspectos legais, mas também um conhecimento técnico sobre os aspectos da segurança cibernética.

2.3 CRIMES CIBERNÉTICOS MAIS COMUNS: FRAUDES ELETRÔNICAS, INVASÕES DE SISTEMAS, ROUBO DE INFORMAÇÕES PESSOAIS, DIFAMAÇÃO ONLINE

Os crimes cibernéticos assumem várias formas, refletindo a ampla gama de atividades que agora ocorrem online. Algumas das formas mais comuns de crimes cibernéticos incluem fraudes eletrônicas, invasões de sistemas, roubo de informações pessoais e difamação online.

Fraudes eletrônicas estão entre os crimes cibernéticos mais comuns. Tais crimes envolvem o uso de computadores ou da Internet para enganar as vítimas e obter dinheiro ou informações valiosas de forma ilegal. O phishing é uma forma comum de fraude eletrônica, na

qual os criminosos se passam por uma entidade confiável para enganar as vítimas e obter suas informações pessoais ou financeiras (ALMEIDA, 2023).

Invasões de sistemas, também conhecidas como hacking, envolvem o acesso não autorizado a sistemas ou redes de computadores, muitas vezes com o objetivo de roubar informações ou causar danos (SILVA,2017)). A invasão de sistemas é um crime sério, pois pode levar à perda ou corrupção de dados, interrupção dos negócios e violações da privacidade.

O roubo de informações pessoais é outra forma comum de crime cibernético. Isso ocorre quando os criminosos obtêm informações pessoais, como nomes, endereços, números de segurança social e detalhes de cartões de crédito, geralmente com o objetivo de cometer fraudes de identidade (PEREIRA, 2022).

A difamação online é um crime cibernético que envolve a publicação de informações falsas ou enganosas sobre uma pessoa na Internet com a intenção de prejudicar a reputação dessa pessoa. Devido à natureza global e permanente da Internet, a difamação online pode ter consequências graves e duradouras para as vítimas (BATISTA, 2020).

2.4 MEDIDAS DE PREVENÇÃO E CONSCIENTIZAÇÃO SOBRE CRIMES CIBERNÉTICOS

A prevenção e a conscientização sobre crimes cibernéticos são fundamentais para proteger indivíduos e organizações contra ameaças online. Existem várias estratégias que podem ser adotadas para combater crimes cibernéticos, desde a educação e conscientização até a implementação de controles técnicos de segurança.

Segundo De Rê (2021) a educação e a conscientização sobre segurança cibernética são algumas das estratégias de prevenção mais eficazes. É importante que os usuários da Internet estejam cientes dos riscos associados às atividades online e das medidas que podem tomar para proteger suas informações. A conscientização sobre segurança cibernética deve ser uma parte essencial da educação digital, desde a escola até o local de trabalho.

Além da conscientização, é crucial que sejam implementadas medidas técnicas de segurança para proteger contra ameaças cibernéticas. A implementação de controles de segurança, como firewalls, antivírus e criptografia, pode ajudar a proteger sistemas e redes contra-ataques cibernéticos. Além disso, a detecção e resposta a incidentes, que envolve o monitoramento de sistemas para identificar possíveis ataques e responder a eles de maneira rápida e eficaz, é um componente crítico da prevenção de crimes cibernéticos (BANDEIRA *et al.*, 2023).

Outra estratégia importante de prevenção de crimes cibernéticos é a implementação de políticas de segurança cibernética. Como Filgueiras e Lima (2015) observam, as políticas de segurança cibernética definem as regras e procedimentos que os usuários de uma rede ou sistema devem seguir para garantir a segurança. Essas políticas podem incluir requisitos para senhas fortes, limitações sobre o uso de dispositivos pessoais no trabalho e orientações sobre como responder a e-mails suspeitos.

Além disso, a colaboração entre organizações, tanto no setor público quanto no privado, é vital para prevenir crimes cibernéticos, a troca de informações sobre ameaças cibernéticas entre organizações pode ajudar a prever e prevenir ataques.

2.5 DESAFIOS ENFRENTADOS NA REGULAMENTAÇÃO PENAL DE CRIMES CIBERNÉTICOS

A regulamentação penal de crimes cibernéticos apresenta vários desafios. A natureza global da internet, a velocidade das mudanças tecnológicas e a complexidade da atribuição de responsabilidade são algumas das questões que tornam a regulamentação de crimes cibernéticos uma tarefa complexa.

Os crimes cibernéticos muitas vezes envolvem atores de diferentes jurisdições, o que dificulta a investigação e a acusação desses crimes. Além disso, as diferenças nas leis e regulamentos de diferentes países podem criar brechas legais que os criminosos cibernéticos podem explorar (BANDEIRA *et al*., 2023).

A velocidade da mudança tecnológica é outro desafio significativo. As leis e regulamentos precisam acompanhar o ritmo das novas tecnologias e das novas formas de crime cibernético que elas possibilitam. Como observado por Wall (2007), a lei muitas vezes luta para acompanhar o ritmo da mudança tecnológica, tornando difícil prevenir e punir efetivamente os crimes cibernéticos.

A complexidade da atribuição é outro obstáculo na regulamentação penal de crimes cibernéticos. Determinar quem é responsável por um crime cibernético pode ser difícil devido ao anonimato que a internet proporciona.

2.6 O IMPACTO DOS CRIMES CIBERNÉTICOS NA VIDA DAS VÍTIMAS E A NECESSIDADE DE SUPORTE

Os crimes cibernéticos podem ter um impacto significativo na vida das vítimas, gerando tanto danos materiais quanto emocionais. Os danos podem variar dependendo da natureza do crime, mas geralmente incluem perda financeira, danos à reputação, violação da privacidade e

angústia psicológica (SILVA, 2017).

A perda financeira é uma das consequências mais diretas e imediatas dos crimes cibernéticos. Como apontado por Wall (2007), as vítimas de fraudes online, roubo de identidade e outros tipos de crimes cibernéticos financeiros podem enfrentar perdas financeiras significativas.

Além da perda financeira, os crimes cibernéticos também podem resultar em danos à reputação das vítimas. Isso é especialmente verdadeiro no caso de crimes como difamação online e vazamento de informações pessoais. A reputação de uma pessoa ou empresa pode ser seriamente prejudicada por esses crimes, com efeitos potencialmente duradouros.

A violação da privacidade é outra consequência grave dos crimes cibernéticos. Como observado por Hildebrandt (2015), crimes cibernéticos como o *hacking*, o *phishing* e o vazamento de dados podem violar a privacidade de uma pessoa, expondo informações pessoais e sensíveis.

Tudo isso destaca a necessidade de fornecer suporte adequado às vítimas de crimes cibernéticos. Isso pode incluir aconselhamento, assistência jurídica, apoio financeiro e serviços de recuperação de identidade. Também é importante conscientizar as pessoas sobre os riscos dos crimes cibernéticos e as medidas que podem tomar para se proteger.

2.7 O FUTURO DO DIREITO DIGITAL: DESAFIOS E PERSPECTIVAS

O Direito Digital é um campo em rápida evolução, moldado por inovações tecnológicas e mudanças no comportamento dos usuários. Diversos desafios e perspectivas emergem em relação ao futuro deste ramo jurídico.

Um dos desafios principais é a velocidade da inovação tecnológica. Como observado por Rogers (2017), a lei geralmente luta para acompanhar a rapidez com que a tecnologia e o comportamento online estão mudando. Isso cria uma lacuna onde novas formas de comportamento prejudicial ou criminoso podem surgir antes que a lei tenha tempo de se adaptar.

Outro desafio importante é a natureza global da internet, a internet não respeita fronteiras nacionais, o que pode tornar difícil a aplicação de leis e regulamentos nacionais. Isso destaca a necessidade de uma cooperação internacional mais forte no campo do Direito Digital.

Outro desafia a se ressaltar é a questão da responsabilização. Embora a implementação da lei tenha trazido mais segurança às empresas, ela também introduz mecanismos de responsabilização com o objetivo de punir aqueles que não cumprem adequadamente as regras. Dessa forma, a aplicação da LGPD não apenas apresenta desafios, mas também se torna uma

poderosa ferramenta na luta contra eles.

Destarte, ainda que exista outros desafios não citados no presente estudo que devem ser superados para combater efetivamente esse tipo de conduta ilícita dentro do novo panorama legislativo, é crucial começar promovendo uma conscientização entre as partes envolvidas, a fim de garantir que elas compreendam plenamente suas responsabilidades e as diretrizes estabelecidas pela lei.

No entanto, também existem perspectivas promissoras para o futuro do Direito Digital. Por exemplo, o desenvolvimento de "leis inteligentes" que são capazes de se adaptar automaticamente às mudanças na tecnologia e no comportamento online é uma possibilidade empolgante. Isso poderia ajudar a fechar a lacuna entre a velocidade da mudança tecnológica e a capacidade da lei de responder (ROGERS, 2017).

Além disso, a crescente consciência da importância da privacidade online e da segurança dos dados poderia levar a um fortalecimento da legislação e da regulamentação nesses campos. Isso é especialmente relevante à luz de desenvolvimentos recentes, como a aprovação da Lei Geral de Proteção de Dados no Brasil.

No geral, o futuro do Direito Digital provavelmente será caracterizado por desafios contínuos, mas também por avanços promissores. A capacidade dos legisladores e reguladores de responder eficazmente a esses desafios e aproveitar essas oportunidades será crucial para moldar o futuro deste campo jurídico importante.

3 METODOLOGIA

O presente estudo foi construído a partir de uma revisão da bibliográfica, baseada em um estudo descritivo, para tanto foram analisados artigos publicados nas principais bases de dados voltados para utilização das TIC’s para o cibercrime.

No que concerne ao tipo de estudo, pode-se dizer que se tratou-se de um estudo qualitativo, uma vez que tem como objeto estudos previamente disponíveis nas principais bases de dados. Cabe ainda salientar que uma revisão da literatura pode ser dividida em várias etapas distintas, podendo assim descrever a aplicabilidade e seus critérios.

Para a construção de uma revisão da literatura é necessário que haja a reunião de hipóteses, que visam responder uma questão central, onde o tema foi delimitado para entender acerca da utilização das novas tecnologias na criminalidade. Logo, o presente estudo buscou responder a seguinte questão norteadora: A falta de regulamentação e controle adequados das TIC’s pode contribuir para o aumento da criminalidade?

Após a escolha do tema de um estudo e a formulação da questão norteadora da pesquisa, com busca nas bases de dados, analisando os estudos que foram inclusos na revisão. Assim, pode-se dizer que a internet é considerada como uma importante ferramenta na seleção dos estudos e para uma análise crítica, assim este instrumento é fundamental para se obter a validade da revisão, bem como funcionar como um indicador de confiabilidade, amplitude e poder de generalização das conclusões da revisão.

Para a busca dos estudos foram utilizados os seguintes descritores: cibercrime. Legislação, TIC's. As estratégias de busca foram baseadas em língua vernácula através da utilização do operador booleano AND. As fontes utilizadas para reunir os artigos serão: SciElo e Google acadêmico. O recorte temporal se dará nos últimos 10 anos, porém deu-se preferência para estudos mais recentes, ou seja, utilizando os artigos dos últimos 5 anos.

Ainda acerca dos critérios de inclusão para a seleção dos artigos, podemos dizer que: publicados em português, que estiverem na integra com versão gratuita disponível. Foram excluídos do estudo artigos que não atendessem os critérios elucidados pela presente metodologia.

4 CONSIDERAÇÕES FINAIS

Em conclusão, as regulamentações penais em crimes cibernéticos desempenham um papel crucial na proteção da sociedade no mundo digital. Com o aumento dos crimes cibernéticos e a rápida evolução da tecnologia, é essencial ter leis e regulamentações atualizadas que abordem essas ameaças de maneira eficaz.

Através dessas regulamentações, crimes como *hacking*, fraudes eletrônicas, roubo de dados e invasões de privacidade são definidos como delitos, permitindo a investigação, o julgamento e a punição dos infratores. Isso estabelece uma base legal sólida para responsabilizar os criminosos cibernéticos e dissuadir outros potenciais infratores.

Além disso, as regulamentações penais em crimes cibernéticos promovem a cooperação internacional, reconhecendo a natureza transnacional desses crimes. Através de acordos e tratados internacionais, os países podem compartilhar informações, extraditar criminosos e trabalhar juntos para combater o cibercrime de forma eficaz.

No entanto, existem desafios significativos na aplicação dessas regulamentações, como a natureza anônima da internet e a evolução constante das táticas de ataque. É importante que as regulamentações sejam flexíveis e atualizadas para enfrentar esses desafios em constante mudança.

Além das regulamentações penais, a conscientização e a educação são fundamentais para combater os crimes cibernéticos. Os usuários devem ser informados sobre os riscos associados ao uso da tecnologia e as melhores práticas de segurança digital. As regulamentações podem incluir disposições para promover a conscientização e a educação da população, fortalecendo assim a proteção no mundo digital.

Em suma, as regulamentações penais em crimes cibernéticos são essenciais para proteger a sociedade no ambiente digital. Elas definem os crimes, estabelecem penas apropriadas, promovem a cooperação internacional e buscam garantir a segurança e a privacidade no mundo digital em constante evolução. No entanto, é necessário um esforço contínuo de governos, órgãos de aplicação da lei, especialistas em tecnologia e setor privado para enfrentar os desafios emergentes, aprimorar continuamente as regulamentações relacionadas ao Direito Digital e Tecnologia e especialmente novos estudos sobre a temática em questão.

REFERÊNCIAS

ALVES, Sabrina Sousa de Andrade. **Pornografia não consensual: uma nova modalidade de violência de gênero e a ausência de legislação penal específica referente ao tema**. 2017.

BANDEIRA, Cauê da Silva et al. **Segurança em redes de computadores: medidas para detecção e prevenção de ataques cibernéticos em redes corporativas**. 2023.

BATISTA, Emerson O. **Sistemas de informação**. Saraiva Educação SA, 2017.

BATISTA, Nathalia Kellen Lemos. **Cibercrimes na internet: uma análise dos reflexos e consequências da vida offline.** 2020.

BOHRER, Igor Graeff et al. **A proteção de dados pessoais como direito da personalidade e seu risco diante do online profiling.** 2019.

BRASIL. DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 28 de set. 2023.

BRASIL. **Lei 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 28 de set. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso de internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 28 de

set. 2023.

CRESPO, Marcelo. **As Leis nº 12.735/2012 e 12.737/2012 e os crimes digitais: acertos e equívocos legislativos**. Abr 2015.

DA SILVA, Michel Bernardo Fernandes. **Cibersegurança: Visão Panorâmica Sobre a Segurança da Informação na Internet**. Freitas Bastos, 2023.

DANIEL, Maycon Antônio et al. **A evolução e aplicação da segurança da informação por meio da lei geral de proteção de dados pessoais (lgpd): um estudo de caso em uma instituição financeira.** 2022.

DE RÊ, Eduardo et al. **Ciberespaço e segurança cibernética: as estratégias cibernéticas de EUA, China e Israel e as suas relações com a estratégia cibernética do Brasil.** 2021.

DOS SANTOS, Liara Ruff; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. **Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo**. 2017.

FILGUEIRAS, Isadora C. A; LIMA, Thais S. Cibercrime. In: ETIC, 2015, Presidente Prudente. **Anais do Encontro Toledo de Iniciação Científica Prof. Dr. Sebastião Jorge Chammé.** Intertemas Toledo Prudente, Presidente Prudente, v. 11, n. 11, 2015.

GALINDO, Guilherme Delgado. **Evolução do estelionato pelo meio digital**. 2022.

HILDEBRANDT, M. Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. **Edward Elgar Publishing,** 2015.

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

JULIANI, Samuel Nunes et al. **Softwares forenses direcionados à investigação de crimes virtuais em redes de computadores**. 2017.

LARA, Marcelo D.'Angelo. **Discussões sobre direito penal digital na contemporaneidade**. Editora Dialética, 2021.

NOBREGA, Eduardo de Medeiros et al. **Direito à liberdade de expressão versus direito à informação: em busca da construção da cidadania e da compreensão esclarecida na democracia brasileira**. 2021.

OTSU, Denise et al. **Crimes cibernéticos e os limites da liberdade de expressão nas redes.** 2023.

PADOVEZ, Rafael Silva; DO PRADO, Florestan Rodrigo. O direito penal brasileiro no contexto dos crimes cibernéticos. **ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498**, v. 15, n. 15, 2019.

PEREIRA, Valéria de Oliveira Machado. **ESTELIONATO VIRTUAL: O click do crime.** 2022.

PINHEIRO, Patrícia Peck. **Direito digital**. Saraiva Educação SA, 2021.

REIS, Érika Lousano Sanchez. **Crimes Digitais Impróprios: Uma Abordagem Constitucional e Crítica Diante da Violação de Direitos Alheios; Insegurança na Legislação Vigente e a (Falta de) Interpretação de Texto no Âmbito Digital**. Editora Appris, 2021.

ROGERS, David L. **Transformação digital: repensando o seu negócio para a era digital**. Autêntica Business, 2017.

SILVA, Ana Laura R. **Cibercrimes: uma análise sob a perspectiva da aplicação do direito internacional.** 2019. 30 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Uberlândia, Minas Gerais, 2019.

SILVA, K. B; CAVALCANTI, G. H. L. **Criminalidade na era da informação: definições sobre criminalidade complexa.** Revista de Direito, Governança e Novas Tecnologias. Curitiba, v. 2, n. 2, p. 75-93, Jul/Dez, 2016.

SILVA, Remy Gama. Crimes da informática. **Science**, v. 60, 2000.

SILVA, Vanderlei Darlei. **Segurança de redes: mitigação e análise de vulnerabilidades**. 2017.

TOMÉ, Paulo Sérgio et al. **O uso da internet e novas tecnologias numa sociedade conectada: possibilidades, desafios, perigos à luz da ética**. 2018.

WALL, D. S. Cybercrime: The transformation of crime in the information age. **Polity**, 2007