RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

CRIMES CIBERNÉTICOS E INVASÃO DE REDES SOCIAIS

CYBERCRIME AND INVASION OF SOCIAL NETWORKS

CIBERCRIMEN E INVASIÓN DE REDES SOCIALES

Adeliane Siqueira Picoli Martins[1], Alexandre dos Santos[1], Juan Silva Nunes[1], Walewska Caravelas Dias[1]

e5105810
https://doi.org/10.47820/recima21.v5i10.5810

PUBLICADO: 10/2024

RESUMO
Este trabalho visa alertar sobre o aumento de invasões a contas e espionagem de redes sociais, resultando em transtornos pessoais, como a exposição da vida privada e até chantagens financeiras. Esses crimes cibernéticos afetam também a vida familiar e profissional das vítimas. A pesquisa analisa a legislação atual e como a população pode se proteger. Para isso, foram utilizados dados de ocorrências registradas, matérias jornalísticas, estatísticas e informações da Anatel e da empresa de proteção de dados Akamai. O estudo revela 1,6 bilhão de casos de roubo de dados pessoais. Além de examinar o impacto desse tipo de crime, o trabalho questiona a eficácia da legislação vigente e propõe medidas de proteção e atualização das leis para acompanhar o avanço das ameaças cibernéticas.

PALAVRAS-CHAVE: Crimes. Cibernético. Roubo. Redes Sociais.

ABSTRACT
This paper aims to raise awareness about the increase in account invasions and social media espionage, leading to personal disruptions such as the exposure of private life and even financial blackmail. These cybercrimes also impact the victims' family and professional lives. The research analyzes current legislation and how the population can protect itself. Data from recorded incidents, news reports, statistics, and information from Anatel and the data protection company Akamai were used. The study reveals 1.6 billion cases of personal data theft. In addition to examining the impact of these crimes, the paper questions the effectiveness of current legislation and proposes protective measures and updates to laws to keep up with the evolution of cyber threats.

KEYWORDS: *Crimes. Cyber. Theft. Social Media.*

RESUMEN
Este trabajo tiene como objetivo alertar sobre el aumento de las invasiones a cuentas y el espionaje en redes sociales, lo que resulta en trastornos personales, como la exposición de la vida privada e incluso chantajes financieros. Estos delitos cibernéticos también afectan la vida familiar y profesional de las víctimas. La investigación analiza la legislación actual y cómo la población puede protegerse. Para ello, se utilizaron datos de incidentes registrados, artículos periodísticos, estadísticas e información de Anatel y de la empresa de protección de datos Akamai. El estudio revela 1,6 mil millones de casos de robo de datos personales. Además de examinar el impacto de este tipo de delito, el trabajo cuestiona la eficacia de la legislación vigente y propone medidas de protección y actualización de las leyes para seguir el avance de las amenazas cibernéticas.

PALABRAS CLAVE*: Delitos. Cibernético. Robo. Redes Sociales.*

INTRODUÇÃO

A cibernética é a ciência da comunicação e do controle, seja nos seres vivos, ou seja, nas máquinas. A comunicação é a ferramenta que torna os sistemas integrados e coerentes e o controle é

[1] Graduanda (o) em Direito. UNIVC - Instituto Vale do Cricare.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

que regula o seu comportamento (Neto, 2017). Segundo Wiener (1948), a cibernética tem um papel fundamental na inter-relação entre comunicação e controle. A cibernética compreende os processos físicos, fisiológicos, psicológicos etc., de transformação da informação (Bernardes, 2021). De acordo com Castells (2009), essa ciência é essencial para o desenvolvimento das novas tecnologias.

Ela visa proteger as pessoas e empresas contra os ataques cibernéticos, que se aproveitam das vulnerabilidades das redes digitais para invadir, roubar e manipular dados e informações (Nascimento, 2018). Conforme Choucri (2012), essas vulnerabilidades cibernéticas crescem à medida que mais sistemas são conectados à internet.

A revolução digital tem transformado profundamente a sociedade. Bilhões de pessoas, nas últimas duas décadas, se beneficiaram da rápida adoção dos recursos de tecnologia da informação, da comunicação, do crescimento exponencial do acesso à internet e das oportunidades econômicas e sociais oriundas do ambiente digital Martins (2015). Os rápidos avanços na área de tecnologia da informação e comunicação resultaram no uso intenso do espaço cibernético para as mais variadas atividades, inclusive o roubo de dados, senhas e invasões de redes sociais Lemos (2020).

Novas e crescentes ameaças cibernéticas surgem na mesma proporção que os meios de comunicação social evoluem, colocando em risco a administração pública e a sociedade Silva (2019). Desse modo, proteger o espaço cibernético requer visão atenta e liderança para gerenciar mudanças contínuas, políticas, tecnológicas, educacionais, legais e internacionais (Diário Oficial da União, 2020). Nesse sentido, o Governo, a indústria, a academia e a sociedade em geral devem incentivar a inovação tecnológica e a adoção de tecnologias de ponta para manter constante atenção à segurança nacional, à economia e à livre expressão (Nielsen, 2022).[1]

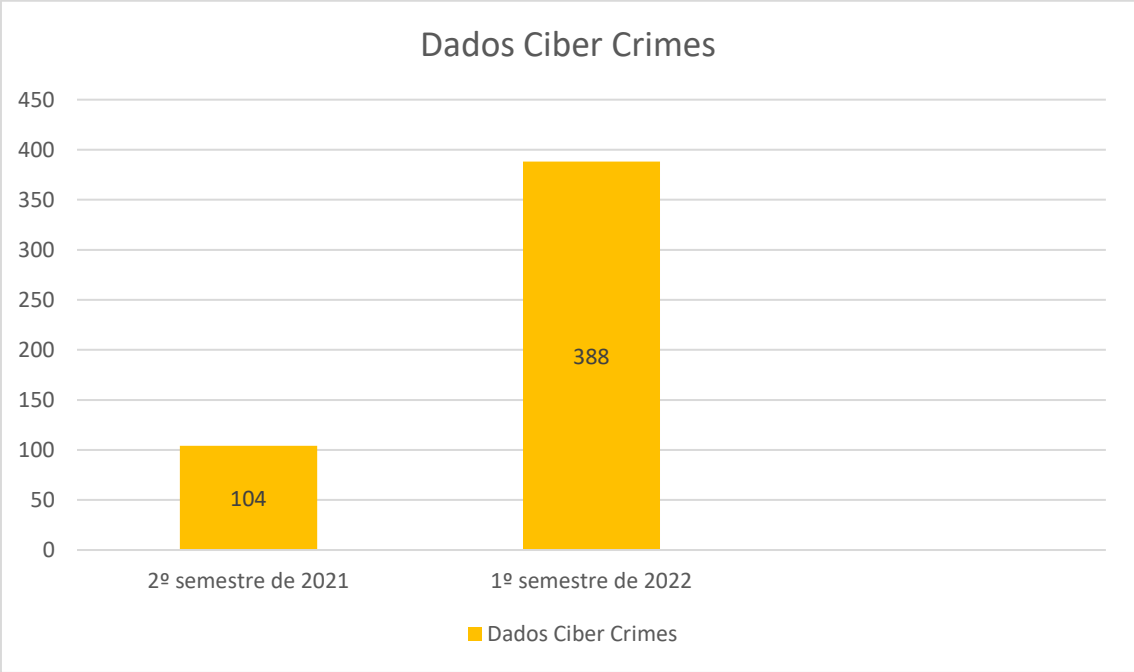
MÉTODOS

O estudo possui natureza quantitativa, visando argumentar os resultados por meio de análises e percepções. A Metodologia utilizada neste trabalho incluiu analisar dados estatísticos e leis já existentes. Em Minas Gerais, por exemplo, casos de crimes cibernéticos cresceram quatro vezes em relação à média do segundo semestre de 2021, conforme aponta o Ministério Público (MP) mineiro. A invasão de perfis na rede social Instagram entrou no radar do MP, depois que os casos de crimes cibernéticos cresceram 273% em comparação à média do segundo semestre de 2021, quando foram somados 104 casos por mês, chegando a 388 ocorrências em janeiro de 2022.

[1] Decreto Nº10.222 de 05/02/2020

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Gráfico 1 – Comparação ciber crimes entre 2021 e 2022



Fonte – Ministério Público de Minas Gerais

O alerta sobre a segurança digital foi emitido em 08 de fevereiro de 2022, durante a celebração do Dia da Internet Segura, uma data dedicada à conscientização das pessoas sobre o uso responsável e seguro dos meios digitais. De acordo com Mauro Ellovitch, promotor de Justiça e coordenador da Coeciber, alertar a população nesse contexto é essencial, pois os crimes cibernéticos vêm crescendo, causando sérios prejuízos para os usuários da internet. Ellovitch destacou que o Ministério Público (MP) tem atuado intensamente na prevenção desses crimes e na punição dos responsáveis, pois muitas vítimas relatam, além de prejuízos financeiros, ameaças e chantagens feitas pelos criminosos (Ellovitch, 2022, p. 12).

Ainda segundo Ellovitch (2022), uma das formas mais comuns de apropriação de perfis no Instagram é por meio de *"phishing"* ou engenharia social, onde os criminosos enviam mensagens diretamente pelo Instagram, WhatsApp, SMS ou *e-mail.* Essas mensagens geralmente oferecem prêmios ou descontos, como em restaurantes, hospedagem ou milhas aéreas, ou até falsas verificações de contas para influenciadores digitais. Em alguns casos, as ofertas falsas se referem a locais que a própria vítima marcou em seu perfil, o que aumenta a credibilidade do golpe (Ellovitch, 2022, p. 13).

Junto com a mensagem ou na sequência do diálogo, os criminosos enviam um link. Quando a vítima clica no *link,* um programa malicioso tem acesso aos dados do titular da conta. Se os golpistas não possuem esses programas, eles pedem que a própria vítima forneça dados sobre sua conta no

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Instagram em uma mensagem que ela receberá por SMS. Essa mensagem, na verdade, é o código de recuperação de senha da conta do Instagram.[2]

Com os dados obtidos através de hackeamento ou fornecidos diretamente pela vítima, os criminosos conseguem acessar o perfil da rede social, modificando a senha e os dados de verificação, o que resulta na perda de controle da conta pelo verdadeiro titular. Com o perfil sob controle, os infratores começam a postar ofertas de produtos como celulares, geladeiras, móveis, entre outros, a preços abaixo do mercado, simulando ser o proprietário legítimo da conta. Nessas postagens, alegam que estão vendendo os itens com urgência ou realizando grandes liquidações. Os seguidores da conta, ao acreditarem na veracidade da oferta, entram em contato e transferem dinheiro para chaves Pix fornecidas pelos criminosos (Coeciber, 2022, p. 15). Em alguns casos, os golpistas chegam a exigir pagamentos para devolver a conta, especialmente quando se trata de perfis profissionais.

No intuito de prevenir novos crimes, a *Coeciber* recomenda que os usuários não cliquem em *links* suspeitos enviados via Instagram, WhatsApp, SMS ou e-mail, pois podem conter programas maliciosos capazes de capturar dados e senhas. Além disso, é importante evitar fornecer dados pessoais a desconhecidos em conversas *online.* A verificação em duas etapas deve ser ativada no Instagram, preferencialmente com aplicativos de autenticação, como Google *Authenticator* ou Microsoft *Authenticator*, em vez de SMS, para aumentar a segurança (Coeciber, 2022, p. 17). Outra recomendação inclui a remoção do número de telefone vinculado à conta, substituindo-o por e-mail ou outra informação pessoal.

A desconfiança de ofertas muito atrativas em perfis que anteriormente não comercializavam produtos é essencial, principalmente quando os preços estão bem abaixo do mercado. Nesses casos, há uma grande probabilidade de fraude. Para evitar prejuízos, o Ministério Público (MP) sugere que os pagamentos não sejam realizados por meio de depósitos ou Pix para terceiros e alerta para a importância de conscientizar familiares, sobretudo os mais idosos, sobre esses crimes (Coeciber, 2022, p. 19).

Relatórios recentes indicam que, em 2020, o Brasil ocupou o terceiro lugar mundial em ataques cibernéticos voltados ao roubo de credenciais, segundo a empresa Akamai. Foram registrados 1,6 bilhão de casos de roubo de dados pessoais na internet, o que ressalta a importância de os usuários frequentarem apenas sites confiáveis e evitarem mensagens suspeitas (Akamai, 2020, p. 22).

Ao longo de 2020, a Akamai Technologies detectou mais de 3 bilhões de tentativas de roubos de credenciais no Brasil. Mais da metade das ocorrências, 1,6 bilhão, tiveram origem no próprio país. O recorde diário ocorreu no mês de dezembro, com mais de 55 milhões de tentativas de fraudes em um só dia.

Serviços financeiros, no entanto, representaram uma pequena parcela dos alvos nessa modalidade de fraude, com pico de 1.1 milhão de tentativas de roubo de credenciais em um único dia ao longo de 2020.

[2] Jornal Tribuna de Minas, matéria de Marcos Araújo, 08/02/2022.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Alguns setores já possuem estruturas mais maduras para identificar e combater esses crimes, mas empresas de todos os portes devem ficar atentos a essa modalidade de crime cibernético e fornecer ambientes seguros para seus clientes por meio de soluções de tecnologia. Aos usuários, as verificações em duas etapas e a variedade e rotatividade de senhas é a melhor prevenção.

O aumento de ataques cibernéticos em 2020 alerta para deficiência em sistemas de prevenção e segurança digital. A necessidade do afastamento social causada pela pandemia de Covid-19 fez com que o uso da internet aumentasse em mais de 40% no Brasil, segundo dados da Agência Nacional de Telecomunicações (Anatel).

Em 05 de fevereiro de 2020, o então Presidente da República, Jair Messias Bolsonaro, no uso de suas atribuições, através do Decreto nº 10.222, aprovou a Estratégia Nacional de Segurança Cibernética – E-Ciber, que visa orientar a sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023.

CRIMES DIGITAIS: QUAIS LEIS TIPIFICAM COMO CRIMES?

Em 2012 foram sancionadas duas leis que estabeleceram penalidades para crimes cometidos no ambiente digital, modificando o Código Penal. Essas leis introduziram sanções para práticas como invasão de dispositivos eletrônicos, disseminação de malwares para roubo de credenciais e o uso indevido de dados de cartões de crédito e débito sem o consentimento dos titulares (Silva, 2018, p. 45).

A primeira dessas legislações é a Lei 12.737/2012, mais conhecida como Lei dos Crimes Cibernéticos ou Lei Carolina Dieckmann, que criminaliza ações como invasão de sistemas, acesso não autorizado a informações pessoais e a derrubada intencional de *websites.* Embora a lei tenha se popularizado após o caso da atriz Carolina Dieckmann, em que fotos pessoais foram divulgadas sem permissão, o projeto já era uma demanda antiga do setor financeiro, preocupado com o aumento de fraudes e furtos de dados pela internet (Santos, 2020, p. 32).

A Lei 12.737/2012 trouxe importantes avanços ao tipificar condutas criminosas que até então não eram devidamente regulamentadas no Brasil. De acordo com Souza (2019), essa legislação foi essencial para proporcionar maior proteção aos usuários da internet, uma vez que estipula penas de detenção para quem invadir dispositivos alheios, alterando ou excluindo dados sem autorização (Souza, 2019, p. 58). A sanção pode variar de três meses a um ano de prisão, além de multa, dependendo da gravidade do delito.

Além disso, a lei também abrange crimes relacionados ao uso indevido de dispositivos eletrônicos para fins ilícitos, como o roubo de senhas bancárias, uma prática comum que afeta milhões de brasileiros anualmente. Conforme Mendes (2021), a aplicação dessa lei tem ajudado a reduzir a sensação de impunidade nos crimes virtuais, embora ainda exista a necessidade de maior fiscalização e atualização constante da legislação para acompanhar o avanço da tecnologia (Mendes, 2021, p. 74).

Paralelamente, a Lei 12.965/2014, conhecida como Marco Civil da Internet, complementou os esforços para regulamentar o uso da rede, estabelecendo direitos e deveres tanto para os usuários

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

quanto para as empresas que fornecem serviços *online*. Segundo Almeida (2020), o Marco Civil é fundamental para garantir a liberdade de expressão e a proteção de dados pessoais, além de definir regras claras para a responsabilidade de provedores de internet em casos de conteúdos ilícitos (Almeida, 2020, p. 102).

> **"Invasão de dispositivo informático**
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Os crimes classificados como menos graves, como a "invasão de dispositivo informático", podem resultar em penas de três meses a um ano de prisão, além de multa. Em situações mais graves, onde a invasão resulta na obtenção de conteúdos como "comunicações eletrônicas privadas, segredos comerciais ou industriais e informações confidenciais", a pena pode variar de seis meses a dois anos de prisão, somada à multa. Segundo Santos (2019), essas punições refletem a crescente preocupação com a privacidade e a segurança de informações no ambiente digital, já que a obtenção e uso indevido desses dados representam sérios riscos tanto para indivíduos quanto para empresas (Santos, 2019, p. 87).

Quando o crime envolve a divulgação, comercialização ou transmissão de dados obtidos de forma ilícita a terceiros, seja por venda ou distribuição gratuita, a pena pode ser agravada em até dois terços. Esse agravante é essencial, conforme Silva (2020), pois visa inibir a circulação de material

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

sigiloso obtido através de invasões, uma vez que a disseminação dessas informações amplia o dano causado à vítima (Silva, 2020, p. 102).

Além disso, a Lei 12.735/2012 tipifica ações que envolvem o uso de sistemas eletrônicos, digitais ou similares com o objetivo de atingir sistemas informatizados, reforçando a necessidade de proteção contra-ataques cibernéticos. Essa legislação também prevê a criação de delegacias especializadas no combate a crimes virtuais, buscando uma atuação mais eficaz na investigação e punição desses delitos (Souza, 2021, p. 134).

ANÁLISE DA ACESSIBILIDADE DAS INFORMAÇÕES LEGAIS SOBRE CRIMES CIBERNÉTICOS E PROPOSTAS PARA AMPLIAR A CONSCIENTIZAÇÃO E PREVENÇÃO ENTRE USUÁRIOS DA INTERNET

Nos últimos anos, o aumento dos crimes cibernéticos tem gerado preocupações significativas entre os usuários da internet. As consequências dessas ações ilegais incluem a invasão de contas pessoais, roubo de dados e chantagens, impactando diretamente a vida cotidiana das vítimas. Apesar da gravidade do problema, a acessibilidade das informações legais que tratam desses crimes ainda é insuficiente, dificultando a compreensão e a reação adequada por parte da população. Essa falta de clareza e divulgação pode ser atribuída a uma série de fatores, incluindo a complexidade das legislações e a carência de campanhas educativas.

De acordo com a Agência Nacional de Segurança (2020, p. 45), "a maioria dos usuários não tem conhecimento sobre as leis que protegem seus dados pessoais e a sua privacidade *online*". Essa falta de informação resulta em um ciclo de vulnerabilidade, onde indivíduos se tornam alvos fáceis para criminosos cibernéticos. A falta de clareza nas legislações e a dificuldade em encontrar informações pertinentes podem levar a uma sensação de impotência entre as vítimas, que muitas vezes não sabem como proceder após sofrer um ataque virtual.

O Marco Civil da Internet (Lei 12.965/2014) e a Lei dos Crimes Cibernéticos (Lei 12.737/2012) são exemplos de legislações que buscam proteger os usuários e punir os infratores. No entanto, conforme observado por Oliveira (2018, p. 312), "a implementação dessas leis enfrenta desafios, pois muitos cidadãos não estão cientes de seus direitos e das ferramentas disponíveis para se protegerem". Isso destaca a necessidade de aumentar a conscientização e promover ações concretas para disseminar informações sobre os direitos e deveres dos internautas.

Para melhorar a acessibilidade das informações legais e a conscientização sobre crimes cibernéticos, algumas ações podem ser implementadas:

1. **Campanhas Educativas:** O governo e as organizações não governamentais (ONGs) devem lançar campanhas educativas, utilizando diferentes mídias (TV, rádio, redes sociais) para informar os usuários sobre como proteger suas informações pessoais e como agir em caso de crimes cibernéticos. Segundo Mendes (2021, p. 59), "as campanhas informativas são essenciais para empoderar os cidadãos a se defenderem no ambiente digital".

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

2. **Treinamentos e *Workshops*:** Instituições públicas e privadas podem oferecer treinamentos e workshops para a população, abordando a legislação relacionada a crimes cibernéticos, as técnicas utilizadas pelos criminosos e as melhores práticas de segurança *online.*

3. **Plataformas de Denúncia:** Criar e promover plataformas digitais acessíveis onde os cidadãos possam reportar crimes cibernéticos de forma simples e rápida. A facilidade de acesso a essas ferramentas é crucial para incentivar as vítimas a buscarem justiça.

4. **Parcerias com Empresas de Tecnologia:** Colaborar com empresas de tecnologia para fornecer recursos e ferramentas que ajudem os usuários a protegerem suas informações. Isso pode incluir a oferta de *softwares* de segurança e a criação de materiais educativos sobre segurança digital.

5. **Aprimoramento da Legislação:** Revisar e atualizar as legislações existentes para torná-las mais compreensíveis e acessíveis ao público em geral. Isso pode incluir a simplificação da linguagem legal e a criação de resumos explicativos que ajudem os cidadãos a entenderem seus direitos.

MARCO CIVIL

O Marco Civil da Internet (Lei 12.965/2014), sancionado em 2014, regulamenta os direitos e deveres dos usuários da internet, protegendo os dados pessoais e a privacidade dos internautas. De acordo com a legislação, apenas com ordem judicial é possível realizar a quebra de sigilo de dados ou acessar informações privadas disponíveis em sites ou redes sociais. A inovação trazida pela lei é crucial para garantir a proteção dos usuários, uma vez que, antes de sua implementação, não havia regulamentação clara sobre procedimentos relacionados à retirada de conteúdo digital, como destaca Lopes (2018), trazendo mais segurança para o ambiente virtual (Lopes, 2018, p. 56).

Um dos aspectos mais importantes é o procedimento para a remoção de conteúdos, que passou a ser feito exclusivamente por ordem judicial, exceto em casos de "pornografia de vingança". Pessoas cujas intimidades foram violadas podem solicitar diretamente aos serviços de hospedagem a retirada de materiais ofensivos, sem a necessidade de um processo judicial inicial. Conforme Lima (2019), essa mudança oferece uma resposta mais ágil às vítimas, uma vez que a disseminação rápida de conteúdos na internet pode causar danos irreparáveis (Lima, 2019, p. 42).

O Conselho Nacional de Justiça (CNJ) também esclarece que o Marco Civil atribui aos Juizados Especiais a competência para julgar casos envolvendo ofensa à honra ou injúria ocorridos na internet, tratadas da mesma forma como as ofensas fora do ambiente virtual. Segundo o CNJ, crimes que envolvem violação de privacidade ou afetam bens e interesses da União ficam sob jurisdição da Justiça Federal, conforme previsto no artigo 70 do Código de Processo Penal (Alves, 2020, p. 87).

Além disso, para combater publicações de cunho homofóbico, xenofóbico, racista ou com conteúdo de pornografia infantil, é possível fazer denúncias anônimas pela plataforma Safernet, que

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

mantém parceria com a Polícia Federal e o Ministério Público Federal. A associação civil, sem fins lucrativos, atua na promoção dos Direitos Humanos e colabora com grandes empresas, como Google, Facebook e Twitter, para garantir a remoção de conteúdos ilegais da internet (Silva, 2021, p. 123).

É considerado crime digital quando o autor atribui a vítima:

*Autoria de um crime sabendo que a vítima é inocente;

*Um fato que ofenda a reputação ou a boa fama da vítima no meio social em que ela vive. Não importa se o fato é verdadeiro.
*Qualificações negativas ou defeitos à vítima.

De acordo com a Delegacia de Repressão aos Crimes Informáticos (DRCI), os crimes mais comuns postados na internet, com o amparo do código Penal.

Ameaça:

> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. (Incluído pela Lei nº 14.132, de 2021)

Calúnia:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
>
> Pena - detenção, de seis meses a dois anos, e multa.
>
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
>
> § 2º - É punível a calúnia contra os mortos.
>
> Exceção da verdade
>
> § 3º - Admite-se a prova da verdade, salvo:
>
> I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
>
> II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
>
> III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Difamação:

Art 139 - Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:

Pena - detenção, de três meses a um ano, e multa.

Exceção da verdade

Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

Injúria:

Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

Pena - detenção, de um a seis meses, ou multa.

§ 1º - O juiz pode deixar de aplicar a pena:

I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;

II - no caso de retorsão imediata, que consista em outra injúria.

§ 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:

Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

§ 3º - Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência: (Redação dada pela Lei nº 10.741, de 2003)

Pena - reclusão de um a três anos e multa. (Incluído pela Lei nº 9.459, de 1997)

Falsa Identidade:

Art. 307 - Atribuir-se para obter vantagem, em proveito próprio ou alheio, ou ou atribuir a terceira falsa identidade para causar dano a outrem:

Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

RESULTADOS E DISCUSSÕES

O presente trabalho tem como objetivo destacar e informar sobre o crescimento significativo de casos envolvendo a invasão de contas de usuários da internet, espionagem de redes sociais e modificação de senhas, os quais geram sérios transtornos na vida pessoal e profissional das vítimas. Entre os impactos identificados estão a exposição da vida privada, casos de chantagem, constrangimentos e solicitações fraudulentas de empréstimos realizados em nome das vítimas, todas ações cometidas por criminosos cibernéticos. Esses atos afetam não apenas a esfera pessoal, mas também a vida profissional, social e familiar das pessoas envolvidas, conforme evidenciado em estudos recentes Silva (2020, p. 45).

Além dos crimes mencionados, casos de roubo de senhas, sequestro de servidores, invasão de páginas e redes sociais e outros cibercrimes vêm sendo relatados com maior frequência. O impacto desses crimes é sentido por diversas vítimas, que podem recorrer ao sistema judiciário para assegurar seu direito à reparação dos danos sofridos. Apesar de ser um tema relativamente novo no contexto legislativo, a crescente quantidade de vítimas e o aumento exponencial desses crimes têm impulsionado a criação e adaptação de leis que buscam acompanhar e regulamentar as novas práticas ilícitas no ambiente virtual Lima (2019, p. 112).

É possível observar que a legislação tem avançado, apresentando textos específicos para abordar cada tipo de crime cibernético. A evolução das normas reflete a tentativa de proteger os usuários de internet e assegurar mecanismos de defesa e reparação para as vítimas. O Marco Civil da Internet (Lei 12.965/2014) e a Lei Carolina Dieckmann (Lei 12.737/2012) são exemplos de marcos legais que visam coibir práticas criminosas e garantir a responsabilização dos infratores Souza (2021, p. 73).

CONSIDERAÇÕES

Diante dos dados apresentados e do contínuo aumento dos crimes cibernéticos, é evidente a vulnerabilidade da população frente a essas ameaças. A sofisticação e a rápida evolução das técnicas utilizadas pelos criminosos digitais, em muitos casos, superam a capacidade das autoridades em acompanhá-las e neutralizá-las de forma eficaz. Embora existam legislações específicas e delegacias especializadas, como as Delegacias de Crimes Cibernéticos, observa-se uma lacuna significativa no acesso e na disseminação de informações de prevenção para o público em geral. Esse cenário reforça a necessidade de uma conscientização mais ampla e acessível sobre os perigos do ambiente digital.

A fragilidade das medidas preventivas, aliada à falta de educação digital em grande parte da população, coloca os indivíduos em risco constante de fraudes, roubos de identidade, ataques de *phishing* e outras formas de crimes virtuais. A prática de verificar cuidadosamente cadastros, links suspeitos e mensagens não solicitadas é crucial para evitar danos financeiros, invasão de privacidade e violações à honra. No entanto, a resposta a esses crimes exige ações rápidas e coordenadas, incluindo o acionamento imediato das Delegacias Especializadas, que possuem o conhecimento

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

técnico necessário para identificar os responsáveis e assegurar que eles sejam penalizados de acordo com a legislação vigente.

A utilização de dados estatísticos sobre crimes cibernéticos tem um papel fundamental no fortalecimento das políticas públicas de segurança digital. Esses dados não apenas embasam a criação de leis mais eficazes, como também servem para mobilizar a sociedade civil e pressionar os legisladores a atualizarem o marco jurídico com maior frequência, garantindo que as novas modalidades de crimes sejam rapidamente enquadradas e punidas. Além disso, a atualização contínua de treinamentos para as autoridades competentes e a implementação de tecnologias avançadas de monitoramento são essenciais para mitigar os impactos desses crimes e aumentar a proteção da população.

Sugestões para Pesquisas Futuras

1. Impacto da educação digital na prevenção de crimes cibernéticos: Um estudo poderia investigar como campanhas educacionais voltadas para a segurança digital influenciam a redução de crimes online, explorando o papel das escolas e organizações públicas na disseminação de boas práticas.
2. Eficácia das delegacias especializadas em crimes cibernéticos: Analisar o desempenho das Delegacias de Crimes Cibernéticos no Brasil, mapeando os desafios que enfrentam e as soluções que têm sido implementadas para melhorar a resposta aos crimes digitais.
3. Desenvolvimento de novas legislações para crimes cibernéticos emergentes: Pesquisar como as legislações existentes se adaptam às novas formas de crimes cibernéticos, como fraudes envolvendo criptomoedas, e propor ajustes legislativos para lidar com essas modalidades.
4. A relação entre tecnologias emergentes e vulnerabilidades cibernéticas: Estudar como o avanço da inteligência artificial, Internet das Coisas (IoT) e outras tecnologias impactam a segurança digital e quais são as novas ameaças que surgem a partir desse contexto.
5. O papel da cooperação internacional no combate aos crimes cibernéticos: Explorar como a colaboração entre países pode ser aprimorada para combater redes criminosas internacionais, que frequentemente operam além das fronteiras nacionais.

REFERÊNCIAS

AGÊNCIA NACIONAL DE SEGURANÇA. **Relatório Anual de Segurança Cibernética 2020**. Brasília: ANS, 2020.

AKAMAI. **Relatório de cibersegurança global 2020**: tendências e ameaças. São Paulo: Akamai Technologies, 2020. 40 p.

ALMEIDA, Carlos. **Marco Civil da Internet**: avanços e desafios. Brasília: Editora Jurídica Nacional, 2020. 150 p.

ALVES, José. **Competências Jurídicas no Marco Civil da Internet**. Rio de Janeiro: Editora Direito & Justiça, 2020. 150 p.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

BERNARDES, Carlos. A cibernética e seus impactos na comunicação moderna. **Revista de Tecnologia**, v. 10, n. 2, p. 23-29, 2021.

BRASIL. **Decreto Nº10.222 de 05/02/2020**. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações**. Estratégia de Segurança da Informação e Comunicações e de Segurança cibernética da Administração Pública Federal**, 2015-2018. Versão 1.0. Disponível em: http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf. Acesso em: maio 2019.

BRASIL. **Decreto-Lei 2.848**. **Código Penal**. Diário Oficial da União, Rio de Janeiro, 11 de Nov, 2021.

CASTELLS, Manuel. **A sociedade em rede**. 5. ed. São Paulo: Paz e Terra, 2009.

CHOUCRI, Nazli. **Cyberpolitics in International Relations**. Cambridge, MA: MIT Press, 2012.

COECIBER. **Prevenção e combate aos crimes cibernéticos no Brasil**. São Paulo: Ministério Público do Estado de São Paulo, 2022. 30 p.

DIÁRIO OFICIAL DA UNIÃO. **Aprova a Estratégia Nacional de Segurança Cibernética.**, [S. l.], 6 fev. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de5defevereirode2020241828419#:~:text=Entretanto%2C%20novas%20e%20crescentes%20amea%C3%A7as,%2C%20educacionais%2C%20legais%20e%20internacionais. Acesso em: 11 maio 2022.

DIÁRIO OFICIAL DA UNIÃO. **Decreto nº 10.222, de 05 de fevereiro de 2020**. Dispõe sobre a Estratégia Nacional de Segurança Cibernética. Diário Oficial da União, Brasília, 2020.

ELLOVITCH, Mauro. **Alerta sobre crimes cibernéticos e estratégias de prevenção**. São Paulo: Ministério Público do Estado de São Paulo, 2022. 20 p.

LEMOS, André. **Comunicação e tecnologia**: riscos cibernéticos na era digital. São Paulo: Intercom, 2020.

LIMA, Maria. **Privacidade e Proteção de Dados na Era Digital**. São Paulo: Editora Jurídica Nacional, 2019. 200 p.

LOPES, Fernanda. **A Regulação da Internet no Brasil**: Análise do Marco Civil. Curitiba: Editora UFPR, 2018. 180 p.

MARTINS, Júlio. **O impacto da revolução digital no Brasil**: uma análise das oportunidades econômicas e sociais. São Paulo: Editora Digital, 2015.

MENDES, Laura. **Cibercrimes no Brasil**: uma análise crítica da Lei Carolina Dieckmann. São Paulo: Editora Jurídica Paulista, 2021. 200 p.

MENDES, R. **Educação e Conscientização sobre Segurança Digital**. São Paulo: Editora Segurança Digital, 2021.

NASCIMENTO, Paula. **Cibersegurança: a proteção no espaço digital**. Rio de Janeiro: Ciência Hoje, 2018.

NETO, Amaury Floriano Portugal. **Teoria da Administração II.** [S. l.], 2017. Disponível em: https://md.uninta.edu.br/geral/teoria-da-administracaoII/files/basic-html/page3.html. Acesso em: 18 maio 2022.

NETO, João. **Cibernética e controle**: ciência da comunicação. Porto Alegre: Editora Sul, 2017.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

NIELSEN, Sarah. **O papel da inovação na cibersegurança global**. São Paulo: Inovatech, 2022.

OLIVEIRA, T. **Crimes Cibernéticos e Legislação**: Desafios e Oportunidades. Rio de Janeiro: Editora Cyberlaw, 2018.

SANTOS, João. **Crimes Cibernéticos e a Legislação Brasileira**. São Paulo: Editora Jurídica Nacional, 2019. 150 p.

SANTOS, Mariana. **Crimes digitais e as novas legislações brasileiras**. Rio de Janeiro: Editora Jurídica, 2020. 120 p.

SILVA, João. **Crimes Virtuais e a Legislação Brasileira**. Recife: Editora Social, 2020. 250 p.

SILVA, João. **Direitos Humanos e Crimes Virtuais**: O Papel da Safernet no Brasil. Recife: Editora Social, 2021. 250 p.

SILVA, João. **Segurança cibernética**: uma análise da legislação brasileira. São Paulo: Revista de Direito e Tecnologia, 2018. 80 p.

SILVA, Mariana. **Proteção de Dados e Privacidade no Ambiente Digital**. Rio de Janeiro: Editora Direito Digital, 2020. 200 p.

SILVA, Roberto. **Ameaças cibernéticas e seus impactos na administração pública**. Brasília: IPED, 2019.

SOUZA, Paulo. **O Marco Civil da Internet e seus Impactos Legais**. Rio de Janeiro: Editora Jurídica Brasil, 2021. 180 p.

SOUZA, Pedro. **Legislação de Crimes Virtuais**: análise e Implementação. Curitiba: Editora UFPR, 2021. 180 p.

SOUZA, Pedro. **Legislação e crimes cibernéticos**: análise da Lei 12.737/2012. Curitiba: Editora UFPR, 2019. 90 p.

STRICKLAND, Fernanda. Estudo aponta 1,6 bilhão de casos de roubo de dados pessoais na internet. **Correio Braziliense**, 2 jun. 2021. Disponível em: https://www.correiobraziliense.com.br/brasil/2021/06/4928596-estudo-aponta-16-bilhao-de-casos-de-roubo-de-dados-pessoais-na-internet.html. Acesso em: 18 maio 2022.

TRIBUNAL REGINAL FEDERAL - 2° REGIÃO. **Crimes diritais:** O que são, como denunciar e quais leis tipificam como crime?. Rio de Janeiro: TRF2, 2018. Disponível em: https://trf2.jusbrasil.com.br/noticias/593431275/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/amp. Acesso em: 17 maio 2022.

WIENER, Norbert. **Cybernetics**: or Control and Communication in the animal and the Machine. New York: MIT Press, 1948.