FACULDADES INTEGRADAS RUI BARBOSA

SARA BAPTISTA MORAES

CRIMES CIBERNÉTICOS NO BRASIL E SUAS CONSEQUÊNCIAS JURÍDICAS

Andradina-SP

Maio 2024

SARA BAPTISTA MORAES

CRIMES CIBERNÉTICOS NO BRASIL E SUAS CONSEQUÊNCIAS JURÍDICAS

Trabalho de conclusão de curso apresentado ao curso de Direito das Faculdades Integradas Rui Barbosa- FIRB, como requisito parcial para à obtenção do título de Bacharela em Direito. Área de concentração: Direito Penal.

Orientador(a): Professora Maria Fernanda Paci Hirata Shimada.

Andradina- SP

Maio/2024

SARA BAPTISTA MORAES

CRIMES CIBERNÉTICOS NO BRASIL E SUAS CONSEQUÊNCIAS JURÍDICAS

Trabalho de Conclusão de Curso apresentado à banca examinadora como requisito parcial para obtenção do Bacharelado em Direito nas Faculdades Integradas Rui Barbosa - FIRB. Defendido e aprovado em _____de _____de _____pela banca examinadora constituída por:

Prof(a). Dr(a). ou Ms. Nome do(a) Orientador(a)_____
Instituição:_____

Prof(a). Dr(a). ou Ms. Nome do(a) Professor(a) Membro_____
Instituição:_____

Prof(a). Dr(a). ou Ms. Nome do(a) Professor(a) Membro_____
Instituição:_____

NOTA: ( ) Aprovado ( ) Reprovado

Andradina, ___de _____de 2024.

Dedico esta monografia primeiramente a Deus, porque sem Ele eu não teria forças e capacidade para desenvolvê-lo. Dedico também a minha mãe, pai e minhas duas irmãs, pois é graças a toda ajuda, esforço e apoio deles que posso concluir o meu curso de Direito; e por fim, a minha professora orientadora Maria Fernanda por ter aceitado a me orientar nesta monografia e os professores restantes por todo aprendizado durante o curso.

“O homem não teria alcançado o possível se, repetidas vezes, não tivesse tentado o impossível.”

Max Weber

RESUMO

A presente monografia tem o intuito de abordar de forma geral os crimes cibernéticos no Brasil, estudando e realizando uma pesquisa frente os impactos e reflexos negativos que causam na sociedade, as dificuldades e desafios enfrentados na investigação, no combate dos crimes e como consequência auxilia no crescimento constante. Além do mais, será abordado no trabalho as formas de regulamentação e dispositivos que tratam sobre os crimes cibernéticos apesar de serem insuficientes devido à grande demanda dos crimes.

Por conta disso, evidenciarei no trabalho a respeito de uma legislação específica dedicada ao tema, com regras claras, precisas e eficazes de modo intuito que promova maior segurança a sociedade no geral e um estudo a respeito desse tipo de delito, com o objetivo de viabilizar o combate, melhorias no processo de investigação e pautar a conscientização da população em relação a segurança na internet.

A metodologia adotada para a realização do estudo foi com base em pesquisa por grandes doutrinadores do Direito Penal, legislações, muita pesquisa sobre o tema, vídeos, jornais, podcasts, leituras de outros trabalhos acadêmicos sobre o assunto, documentários e propagandas sobre o assunto.

Palavras-chave: Crimes cibernéticos. Combate. Investigação.

ABSTRACT

This monograph aims to generally address cybercrimes in Brazil, studying and carrying out research into the negative impacts and reflections they cause in society, the difficulties and challenges faced in the investigation, in combating crimes and, as a consequence, assists in constant growth. Furthermore, the work will address the forms of regulation and devices that deal with cybercrimes despite being insufficient due to the great demand for crimes.
Because of this, I will highlight in the work regarding specific legislation dedicated to the topic, with clear, precise and effective rules intended to promote greater security for society in general and a study regarding this type of crime, with the aim of making it possible the fight, improvements in the investigation process and raising awareness among the population regarding internet security.
The methodology adopted to carry out the study was based on research by great scholars of Criminal Law, legislation, a lot of research on the subject, videos, newspapers, podcasts, readings of other academic works on the subject, documentaries and advertisements on the subject.

Keywords: Cyber crimes. Combat. Investigation.

SUMÁRIO

1 INTRODUÇÃO.....9

2 DA ORIGEM DA INTERNET AOS CRIMES CIBERNÉTICOS.....10

2.1 Histórico e crescimento da internet.....10

2.2 Surgimento e definição de crimes cibernéticos.....12

2.3 Principais tipos penais no meio cibernético.....13

3 CRIMES CIBERNÉTICOS E SUAS IMPLICAÇÕES LEGAIS.....15

3.1 Internet é uma terra sem lei?.....15

3.2 Marco civil da internet (Lei nº 12.965/2014).....15

3.3 Lei Carolina Dieckmann (12.737/2012).....16

3.4 Lei 14.155/21.....17

3.5 A Convenção de Budapeste.....18

3.6 Lei Geral de Proteção de Dados (Lei nº 13.709/2018).....19

3.7 Projeto de Lei das Fake News.....20

4 PANORAMA DOS CRIMES CIBERNETICOS NO BRASIL.....22

4.1 Perfil do criminoso e das vítimas.....22

4.2 Casos famosos e tendências.....24

4.3 Impactos na sociedade.....25

4.3.1 Principais setores críticos.....26

5 PROCEDIMENTOS DE INVESTIGAÇÃO E MEDIDAS DE PREVENÇÃO DOS CRIMES CIBERNETICOS.....28

5.1 Desafios na Investigação 28

5.1.2 Desafio no combate aos crimes cibernéticos.....29

5.2 Como se proteger e denunciar os crimes cibernéticos.....30

6 CONCLUSÃO.....32

REFERÊNCIAS.....33

1 INTRODUÇÃO

A presente pesquisa focará em compreender a relevância dos crimes cibernéticos no Brasil, na qual representa uma realidade cada vez mais presente no cotidiano, com um aumento significativo na incidência de delitos realizados por meio da internet.

Diante desse cenário, é imprescindível entender as consequências jurídicas dessas práticas, tanto em termos de legislação específica quanto de sua aplicação e eficácia no combate dos crimes. Este estudo busca analisar e discutir os desafios enfrentados pelo sistema jurídico brasileiro no enfrentamento dos crimes cibernéticos, também como seus impactos na sociedade.

A questão central do estudo é: Como os desafios e dificuldades em combater e investigar os crimes cibernéticos no Brasil e suas poucas legislações levam a internet ser taxada de “terra sem lei” e como consequência leva a evolução e progresso cada vez mais?.

Então, os passos a serem pesquisados para alcançar a finalidade principal da pesquisa é examinar quais os desafios e dificuldades enfrentados para combater os crimes cibernéticos e seu processo de investigação e averiguar se as normas e diretrizes que são postas para os crimes virtuais são suficientes e eficazes.

Em virtude disso, o presente trabalho foi estruturado em quatro capítulos: O segundo capítulo aborda o histórico e o crescimento da internet, surgimento e definição de crimes cibernéticos e os principais tipos.

No terceiro capítulo, é tratado das implicações legais em relação aos crimes cibernéticos. No quarto capítulo é apresentado um panorama dos crimes virtuais, observando a diferença do perfil do infrator e da vítima, análise de casos famosos, de tendências e os impactos na sociedade.

Por último, o quinto capítulo é exposto os desafios na investigação, no combate e medidas para se proteger e denunciar os crimes cibernéticos.

2 DA ORIGEM DA INTERNET AOS CRIMES CIBERNÉTICOS

Primeiramente, a origem da internet proporcionou inúmeras oportunidades, mas também deu origem a novos desafios, como os crimes cibernéticos. A evolução contínua da tecnologia e da sociedade garantirá que a batalha contra esses crimes permaneça e em constante evolução.

2.1 Histórico e crescimento da Internet

No mês de setembro de 1988, a internet estreou no Brasil, através do Laboratório Nacional de Computação Científica, que se localiza no Rio de janeiro, obteve o acesso à Bitnet, em razão de uma conexão de 9.600 bits por segundo organizado com a Universidade de Maryland (Muller, 2023).

> Algum tempo depois, a Fapesp criou a rede ANSP (Academic Network at São Paulo), interligando a Universidade de São Paulo (USP), a Universidade de Campinas (Unicamp), a Universidade Estadual Paulista (Unesp) e o Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT). Mais tarde, ligaram-se à ANSP a Universidade Federal de Minas Gerais (UFMG) e a Universidade Federal do Rio Grande do Sul (UFRS) (Muller, 2023).

No mês de maio de 1989, Universidade Federal do Rio de Janeiro (UFRJ) passou a integrar a rede Bitnet, por meio da Universidade de Califórnia em Los Angeles (UCLA), tornando-se o terceiro ponto de conexão internacional. Em 1981, foi estabelecido o Ibase (Instituto Brasileiro de Análises Sociais e Econômicas), uma organização autônoma, sem fins lucrativos, que sempre teve nos seus objetivos disseminar informações para a sociedade civil, o que envolvia tornar mais acessíveis a internet no país (Muller, 2023).

> Em meados da década de 80, o Ibase integrou-se a um projeto internacional chamado Interdoc. Sua finalidade era o uso do correio eletrônico para o intercâmbio de informações entre ONGs (organizações não-governamentais) de todo o mundo. Participavam do projeto dezenas de entidades da África, América Latina, Ásia e Europa. Contudo, o uso desse sistema ainda era extremamente caro. Fazia-se necessário encontrar meios alternativos para facilitar essa conexão internacional e reduzir os custos de comunicação. (Muller, 2023).
>
> Alternex, um serviço internacional de mensagens e conferências eletrônicas pioneiro no país. Através do Alternex era possível trocar mensagens com diversos sistemas de correio eletrônico de todo o mundo, incluindo a Internet. O Alternex foi, portanto, o primeiro serviço brasileiro de acesso à Internet fora da comunidade acadêmica (Muller, 2023).

Essa situação perdurou por volta de 1994, quando a Internet saiu dos limites acadêmicos e se popularizou entre muitos brasileiros. Em 17 de julho do mesmo ano, o jornal Folha de São Paulo concedeu a edição dominical ao seu caderno Mais! à "superinfovia do futuro". E declarava: "nasce uma nova forma de comunicação que ligará por computador milhões de pessoas em escala planetária" (Muller, 2023).

> Quase no final de 94, o governo brasileiro - que até então pouco tinha feito pela Internet no Brasil - divulgava, através do Ministério de Ciência e Tecnologia e do Ministério das Comunicações, a intenção de investir na nova tecnologia. A criação da estrutura necessária para a exploração comercial da Internet ficou a cargo da Embratel e da RNP (Muller, 2023).
> No final de 94, a Embratel iniciou seu serviço de acesso à Internet em caráter experimental. Cinco mil usuários foram escolhidos para testar o serviço. Alguns meses depois, em maio de 95, o acesso à Internet via Embratel começou a funcionar de modo definitivo. Mas a exclusividade da Embratel no serviço de acesso a usuários finais desagradou à iniciativa privada. Temia-se que a Embratel e outras empresas de telecomunicações dominassem o mercado, criando um monopólio estatal da Internet no Brasil (Muller, 2023).

De acordo com a pesquisa do IBGE, Nery e Britto (2022) afirmam que “a internet chega a 90,0% dos domicílios do país em 2021, com alta de 6 pontos percentuais frente a 2019, quando 84,0% dos domicílios tinham acesso à grande rede.”

Eles afirmam que “em 2021, pela primeira vez, mais da metade dos idosos acessaram à internet. O percentual de utilização da internet pelas pessoas com 60 anos ou mais de idade saltou de 44,8% para 57,5%, entre 2019 e 2021.”

Entende-se que a expansão do uso da internet vem crescendo com a mudança dos celulares tradicionais para os smartphones. Esses sofisticados aparelhos celulares de última geração permitem o acesso direto à internet em qualquer lugar. Sendo assim, as possibilidades de ingressar na rede mundial de computadores aumentam, consequentemente com o público destinando a um novo cenário a ser explorado e exposto para as práticas de crime virtual (Sérvio, 2021).

Como menciona na pesquisa BBC News Brasil, “Brasil é 2º em ranking de países que passam mais tempo em redes sociais, com 225 minutos, um aumento em relação a 2018, quando o tempo médio gasto com isso foi de 219 minutos” (Brasil..., 2019).

Nos dias de hoje, a internet está tão presente em nossa vida que se tornou indispensável. Atividades como negócios, trabalho, transações, compras, comunicação e entretenimento são realizadas principalmente pela internet, sem contar que com a popularização de redes sociais, como Facebook, Twitter, Instagram, transformou a maneira como as pessoas se comunicam, interagem e trocam informações online, impulsionando ainda mais o crescimento da internet.

2.2 Surgimento e definição de crimes cibernéticos.

O avanço tecnológico e a popularização da internet facilitaram a ocorrências de várias práticas ilícitas no ambiente digital.

> Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata e, acreditando que a internet um espaço livre, acabam por exceder em suas condutas e criando novas modalidades de delito: os crimes virtuais (Pinheiro, 2000).

> O crescente desenvolvimento de tecnologias de informação e o uso massificado da Internet têm facilitado o acesso das pessoas a mais conhecimentos e a processos mais rápidos de tomada de decisões. De outro lado, a informatização tem sido utilizada para fins delituosos, geralmente denominados de "crimes virtuais" ou "cibernéticos". No Brasil, por exemplo, cerca de 3 mil pessoas, por hora, são vítimas de delitos dessa modalidade. Com esses números, o Brasil ocupa o primeiro lugar dentre os países da América Latina, sendo o quarto colocado no mundo (O Senado..., 2012).

Crime cibernético é qualquer ação criminosa que praticada na internet, por meio de dispositivos eletrônicos como computadores, celulares, como meio ou alvo (Nóbrega, 2022).

> Cibercrime é compreendido como a prática de uma conduta ilícita manifestada por meio eletrônico, em que se é utilizado o recurso de Internet como meio para prática delituosa, assim como no envolvimento de arquivos e/ou sistemas digitais. Podem ser cometidos somente em ambiente tecnológico, ocorridos, por exemplo, na manipulação de caixas eletrônicos, ou até mesmo nos crimes convencionais executados na forma digital ou que incluam alguma ação tecnológica para praticar o crime, tendo os crimes contra a honra como exemplificação (Correia, 2020; Fagundes, 2021).

Dickson Cosseti (2020) afirma que "de um modo geral, os tribunais brasileiros adotam como conceito para crime cibernético todo ato que é ilícito, antijurídico culpável e claro, que é cometido via internet."

> Crime de informática é aquele que, quando praticado, utiliza–se de meios informáticos como instrumento de alcance ao resultado pretendido, e aquele praticado contra os sistemas e meios informáticos. Por meios informáticos devemos compreender os hardwares e softwares de computadores, tabletes, smartphones, entre outros dispositivos que possam ser utilizados para a prática delitiva (Teixeira, 2023, p.1160; Aguiar, Neto, Guida, 2023).

No ponto de vista de Cosseti (2020), o objetivo de quem pratica esse tipo de crime é afetar a pessoa da vítima, ou o seu computador, ou uma rede maior de computadores como o caso de

empresas e governos. Ocorre então, que o objetivo é causar algum tipo de transtorno a alguém, prejuízo até financeiro ou até ter algum tipo de vantagem ilícita.

Não existe um consenso sobre a denominação para crimes cibernéticos, pois também são conhecidos como crimes digitais, crimes eletrônicos, crimes virtuais. Porém, no geral todas essas nomenclaturas se denominam no mesmo conceito (Cosseti, 2020).

Os autores Jesus e Milagre (2016), conceituam que crimes virtuais são “fatos típicos e antijurídicos cometidos por meio da ou contra a tecnologia da informação, ou seja, um ato típico e antijurídico, cometido através da informática no geral, ou contra um sistema, dispositivo informático ou redes de computadores.”

Cumpre ressaltar que, com o pensamento de Paz Mendes (2021), são diferenciados os delitos que são cometidos por meio cibernético, daqueles que só podem ocorrer através da tecnologia, como invasão de dispositivos informáticos (qualquer dispositivo eletrônico). Isto é, os primeiros já existiam, sendo ampliado e facilitando apenas o acesso das práticas criminosas. Agora o segundo, passou a existir somente em virtude da tecnologia.

Desse modo, diversos crimes previamente cometidos e reconhecidos, como estelionato, fraudes, desvios, chantagem, assédio, discriminação, crimes contra a honra, entre diversos outros, em decorrência da tecnologia, passaram a ser realizados com mais sofisticação e potência.

2.3 Principais tipos penais no meio cibernético

Há uma pluralidade de crimes cometidos no meio virtual e os tipos penais podem incluir uma variedade de infrações, muitas das quais são similares aos crimes tradicionais, mas cometidos através de meios virtuais.

Como a jornalista Tainá Falcão (2019), alega “crimes como extorsão, calunia, espionagem e até terrorismo atinge cada vez mais usuários da web."

Alguns dos tipos penais comuns nos crimes cibernéticos incluem:

•Calunia: Imputar uma conduta criminosa a alguém

•Injuria: Falar mal, insultar uma pessoa

•Difamação: Associar uma pessoa a um acontecimento que possa “sujar”, denegrir a sua imagem.

•Perfil falso: Criar uma falsa identidade nas redes sociais.

•Acesso em sistemas de computador não autorizados: Entrar ilegalmente em sistemas de computador, redes ou dispositivos móveis sem permissão, muitas vezes com a intenção de roubar informações de forma ilícita ou causar danos.

•Fraude eletrônica: Uso fraudulento de informações eletrônicas para obter vantagens financeiras indevidas, como roubo de identidade, fraude de cartão de crédito, senha bancária, esquemas de phishing e falsificação de documentos eletrônicos.

•Difusão de malware: Criar, distribuir ou implantar software malicioso, como vírus, worms, trojans e ransomware, com o objetivo de danificar sistemas, roubar dados ou extorquir dinheiro.

•Assédio e intimidação online: Comportamento criminoso que envolve ameaças, bullying, stalking ou assédio através de meios digitais, como redes sociais, mensagens instantâneas ou e-mails.

•Estupro virtual: aquele criminoso que teve acesso a alguns dados íntimos de determinada pessoa, e pede determinados favores sexuais em troca de não divulgar os dados.

•Pornografia infantil: Produção, distribuição ou posse de material pornográfico envolvendo menores de idade, seja por meio de troca de arquivos pela internet, compartilhamento em fóruns online ou acesso a sites ilegais.

•Ataques de negação de serviço (DDoS): Sobrecarregar um servidor, rede ou serviço online com tráfego malicioso, tornando-o inacessível para usuários legítimos, com o objetivo de prejudicar a operação normal do sistema.

•Violação de direitos autorais e propriedade intelectual: Distribuição não autorizada de material protegido por direitos autorais, como filmes, música, livros, através da internet.

•Extorsão: Ameaçar divulgar informações confidenciais, fotos intimas ou danificar sistemas de computador, a não ser que seja pago um resgate em criptomoedas ou outra forma de pagamento digital.

•Estelionato: criminoso engana a vítima, induzindo a acreditar em uma mentira, para obter uma vantagem ou benefício para si, ocorrendo através de redes sociais. Muito famoso no Brasil é o “golpe do Whatsapp”, em que números desconhecidos fingem ser um parente próximo da vítima e solicitam favores ou até mesmo dinheiro. (Assis, 2019; Brenol, 2023; Cosseti, 2020; Schwingel, 2020; Stoffel, 2020; Zanolini, 2021; Cordeiro, 2023; Barros, 2024).

Os crimes mais comuns que acontecem no Brasil são o de extorsão, estelionato, difamação, calunia e injuria (D’Úrso, 2019).

3 CRIMES CIBERNÉTICOS E SUAS IMPLICAÇÕES LEGAIS

Neste terceiro capítulo será retratado de alguns dispositivos legais que versam aos crimes cibernéticos.

3.1 Internet é uma terra sem lei?

A natureza da internet pode tornar desafiador aplicar leis e regulamentos de maneira uniforme em todo o mundo. Devido à facilidade de anonimato e à rápida evolução da tecnologia, aplicar a lei na internet pode ser complexo, pois criminosos cibernéticos muitas vezes exploram essas lacunas para praticar atividades ilegais.

> Muitos acreditam que estar escondido por trás de uma tela de computador o torna imune para fazer e dizer o que quiser dentro do mundo digital, praticamente uma terra sem lei. Até pouco tempo atrás, isso era uma meia verdade, pois a regulamentação de ações na internet não era rigorosa e com muitas falhas, dando a falsa sensação de liberdade total, o que inclusive levou à criação de blogs e posts com temáticas racistas e até mesmo com enaltecimento de ideologias criminosas. Com o passar do tempo e com o melhor entendimento da funcionalidade da internet e do poder que ela possui, foram introduzidas, aos poucos, novas formas de regulamentação para que esse ambiente seja seguro para todos, uma vez que a internet é uma extensão da vida real, e, dessa forma, também é passível de aplicação de regras e leis, afinal o direito é um conjunto de regras onipresentes que deve ser aplicado em qualquer camada de realidade, seja física ou digital (A Internet..., 2022).

Infelizmente, na internet tem muito a visão que a internet é um mundo sem lei, podendo fazer o que bem quiser e entender, ficando livre de consequências.

Portanto, enquanto a internet pode parecer em alguns aspectos, uma "terra sem lei", existem sim algumas normas e regulamentos que regem e responsabiliza o comportamento virtual.

No entanto, o cumprimento dessas leis pode ser desafiador e requer esforços de governos, empresas e da sociedade para garantir um ambiente online seguro e legal.

3.2 Marco Civil da Internet (Lei 12.965/2014)

Apenas em 2014, houve a primeira legislação brasileira criada especificamente para regulamentar o uso da internet, a lei 12.965, fazendo parte do conjunto de regulamentações cibernéticas (Viana, 2023).

De acordo com seu artigo 1º da lei, “estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e ainda determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação a matéria.”

Para o jornalista e pesquisador Rodolfo Viana (2023), “o Marco Civil da Internet é a norma legal que disciplina o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem faz uso da rede.”

Nos primeiros artigos, a lei 12.965/2014 aponta os fundamentos, princípios, objetivos e conceitos fundamentais aplicáveis à matéria. É importante ressaltar os princípios que são citados em seu art. 3º que são:

> I - Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - Proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - Preservação e garantia da neutralidade de rede;
> V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - Preservação da natureza participativa da rede;
> VIII - Liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei (Brasil, 2014).

O Marco Civil da Internet está amparado em duas prerrogativas principais sendo a Neutralidade da rede e Privacidade, cujo na primeira não poderá haver diferença no tipo de uso da rede e no segundo diz muito sobre a inviabilidade e sigilo das comunicações online.

3.3 Lei Carolina Dieckmann (12.737/2012)

A legislação conhecida como Lei Carolina Dieckmann, chamada de Lei 12737, contêm quatro artigos e ganhou destaque no Brasil e se tornou importante, por ser uma das primeiras em normatizar e punir os delitos cometidos no meio virtual, ou seja, aqueles praticados por meio de dispositivos eletrônicos e redes de computadores. Antes da promulgação desta Lei, não era considerado ilícito acessar dispositivos privados, sendo enquadrado apenas como atos preparatórios, não sujeitos a penalidades. Porém, com a nova legislação, essa conduta passa a ser tida como crime (Fachini, 2023).

Dessa forma, a sua importância é fundamental para garantir a segurança e privacidade na internet. Além disso, é a legislação responsável por impulsionar o desenvolvimento de outras leis como a Lei Geral de Proteção de Dados e o Marco Civil da Internet (Fachini, 2023).

Esta lei ficou conhecida como "Lei Carolina Dieckmann" devido a um caso específico de violação de privacidade e vazamento de 36 fotos da atriz brasileira Carolina Dieckmann na internet. Na época, o computador da atriz foi invadido por hackers através do e-mail de Carolina e mesmo antes de suas fotos vazarem, os agentes criminosos tentavam chantageá-la, exigindo dinheiro em troca de não as publicar (Fachini, 2023).

> Diante do primeiro escândalo do gênero no país, não tardou para que o caso ganhasse os olhos do público e da justiça. Em menos de um ano após o caso, a lei Nº 12.737/2012, apelidada de Lei Carolina Dieckmann, foi sancionada no dia 30 de novembro de 2012. A criação da lei se deu em virtude do caso da atriz que, na época do crime, não recebeu amparo de uma legislação específica para a devida penalização dos criminosos (Lei..., 2022).
> O novo texto prevê a alteração nos artigos 154-A e 154-B do Código Penal, incluindo, pela primeira vez, a tipificação de crimes virtuais e delitos informáticos, como a invasão de dispositivos informáticos com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do proprietário (Lei..., 2022).

Contudo, a lei tipifica criminalmente os delitos informáticos, na qual inseriu o artigo 154 A do Código Penal sobre a invasão do dispositivo alheio conectado ou não a rede de computadores, por meio de violação de segurança para adulterar ou destruir dados ou informações sem permissão do titular do dispositivo para obter vantagem ilícita, com pena de 3 meses a um ano de prisão e multa (Cabette, 2013).

3.4 Lei 14.155/21

A Lei 14.155/21, conhecida como Lei do Fraude Eletrônica, foi criada para combater crimes cometidos através de meios eletrônicos, com penas mais rígidas para esses tipos de crimes como fraudes pela internet, redes sociais, e-mails, aplicativos e outros meios digitais. Isto significa, que busca gerar uma base legal mais robusta para lidar com crimes denominados “cibernéticos” no Brasil (Milagre, 2021).

A Lei visa atualizar a legislação brasileira para lidar com os desafios e crimes emergentes no ambiente digital.

> A lei 14.155/21 alterou o crime de invasão de dispositivo informático, melhorando sua redação e aumentando substancialmente suas penas (art. 154-A do CP). Além disso, finalmente, foram criados os crimes específicos de furto mediante fraude eletrônica (art. 155, § 4º-B do CP) e de fraude eletrônica (art. 171, § 2º-A do CP) (Barbagalo, 2022).

Como em qualquer legislação, é importante estar ciente de possíveis atualizações ou modificações na aplicação da lei, conforme as mudanças no cenário tecnológico e jurídico do país.

3.5 A Convenção de Budapeste

A Convenção de Budapeste sobre Crime Cibernético é um tratado internacional, adotada em 2001 pelo Conselho Europeu, que visa combater crimes cibernéticos, proteger sociedades contra ameaças virtuais e fortalecer a cooperação internacional nesse ramo (Perícias, 2023).

Na concepção de Felipe Senna e Daniella Ferrari (2020), "a adesão do Brasil à Convenção de Budapeste sobre crimes cibernéticos coincide com a intensa digitalização da vida e o inegável aumento de atividades criminosas cometidas online, inclusive a violação sistemática de direitos autorais."

O intuito consiste em facilitar a colaboração internacional no combate ao crime cibernético. A convenção enfatiza a necessidade de uma política criminal comum, visando resguardar a sociedade contra a delinquência no ambiente virtual, por meio da implementação de leis adequadas e da melhoria da cooperação internacional e encoraja os países signatários a adotarem medidas preventivas, como educação, conscientização e capacitação, para combater o crime cibernético (Cláudio Lima, 2021, p.23).

Adentrando, estabelece mecanismos para a cooperação entre as autoridades judiciais e policiais dos países signatários, incluindo troca de informações e assistência mútua em investigações (Samartini, 2022).

Os principais direitos garantidos pela Convenção de Budapeste são:

> •Direito à liberdade de opinião sem qualquer ingerência;
> •Direito à liberdade de expressão, incluindo a liberdade de procurar, de receber e transmitir informações e ideias de qualquer natureza sem considerações de fronteiras;
> •Direito ao respeito à vida privada (Brasil..., 2021).

> O Brasil foi convidado pelo Conselho da Europa, em 2019, para aderir à Convenção de Budapeste sobre o Crime Cibernético, celebrada em 2001. Nesta semana, o tema foi discutido por especialistas e deputados federais, além de membros do Ministério Público Federal (MPF), durante audiência pública virtual da Comissão de Relações Exteriores e de Defesa Nacional da Câmara. O convite tem validade de três anos, e a mensagem de adesão está em análise na comissão, onde já recebeu parecer favorável de um parlamentar. Caso se comprometa com a Convenção, o Brasil, como Estado Parte, deverá cooperar com a elaboração de leis penais para tipificar os crimes cibernéticos (Brasil..., 2021).

> Outra responsabilidade prevista na Convenção é que os países signatários devem se comprometer a extraditar e a prestar assistência, mesmo que não haja acordos bilaterais, tanto em medidas cautelares quanto em investigações que envolvam crimes

> cometidos em ambientes digitais. Atualmente, o Brasil é apenas observador das regras da Convenção e ainda não tem direito a voto para definição de estratégias e diretrizes. A adesão como membro pleno depende da aprovação do Congresso Nacional, seguida da publicação do decreto legislativo e, por fim, da ratificação pelo chefe do Poder Executivo (ou seja, pelo Presidente da República). O Ministério Público Federal se posicionou também favorável à assinatura do acordo. "Em matéria de crimes cibernéticos, a cooperação internacional precisa ser muito rápida, sob pena de se verem frustrados os esforços para combater a criminalidade, já que as provas eletrônicas podem ser rapidamente eliminadas. Nesse contexto, a adesão à Convenção de Budapeste tornou-se inadiável", defendeu Fernanda Teixeira Souza Domingos, procuradora da República (Brasil..., 2021).

> O Governo Federal promulgou a Convenção sobre o Crime Cibernético, firmada em Budapeste. O Brasil, ao aceitar o convite do Conselho da Europa, passou a ser um dos países que aderiram a tal instrumento internacional multilateral, fortalecendo, assim, os laços de cooperação com parceiros estratégicos no enfrentamento aos crimes cibernéticos. O Decreto nº 11.491, que traz a decisão, foi publicado no Diário Oficial da União (DOU), no dia 12 de abril de 2023. Por meio da denominada Convenção de Budapeste, firmada em 23 de 2001, as autoridades brasileiras poderão contar com mais um recurso nas investigações de crimes cibernéticos, assim como de outras infrações penais, que demandem a obtenção de provas eletrônicas/digitais armazenadas em outros países. Prevê-se uma cooperação "mais intensa, rápida e eficaz" (Convenção..., 2023).

3.6 Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

A Lei Geral de Proteção de Dados (LGPD), oficializada pela Lei nº 13.709/2018, assegura a privacidade e a proteção dos dados pessoais dos indivíduos no Brasil. Esta legislação estabelece diretrizes claras para que as organizações lidem com informações pessoais, promovendo a conscientização em relação à segurança cibernética e incentivando as empresas a implementarem medidas mais robustas de proteção (Eduarda Chaves, 2023).

Um dos postos-chave da LGPD é a exigência de consentimento explícito e específico por parte dos usuários antes da coleta de seus dados, dificultando assim a obtenção ilegal de informações por agentes mal-intencionados. Além disso, a LGPD estipula a adoção de medidas de segurança eficazes pelas empresas, como controle de acesso, criptografia e prevenção contra vazamentos, tornando mais árduo o acesso não autorizado aos dados.

As empresas também são obrigadas a comunicar aos usuários sobre possíveis violações de dados que possam acarretar riscos ou danos, na qual possam ajudar as vítimas a se precaver (Chaves, 2023).

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios (Brasil, 2018).

> A Lei Geral de Proteção de Dados (13.709/2018) tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Também tem como foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes (O que é a LGPD..., s.d.).

> A lei define o que são dados pessoais e explica que alguns deles estão sujeitos a cuidados ainda mais específicos, como os dados pessoais sensíveis e dados pessoais sobre crianças e adolescentes. Esclarece ainda que todos os dados tratados, tanto no meio físico quanto no digital, estão sujeitos à regulação. Além disso, a LGPD estabelece que não importa se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior: se há o processamento de informações sobre pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser observada. A lei autoriza também o compartilhamento de dados pessoais com organismos internacionais e com outros países, desde que observados os requisitos nela estabelecidos (O que é a LGPD..., s.d.).

A proteção de dados tem como princípios:

> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (Brasil, 2018).

3.7 Projeto de Lei das Fake News

De acordo com um estudo conduzido pela Avaaz, 62% dos brasileiros já foram vítimas de alguma fake news, fazendo do Brasil o país mais suscetível a notícias falsas globalmente (Maciel, 2019).

É visível que as fake news estão sempre em alta, tomando grandes proporções e em razão desta, foi iniciado no Senado Federal, o Projeto de Lei nº 2630 que está em andamento desde 2020. Este projeto propõe estabelecer a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet.

Um dos objetivos do PL 2630/2020 incluem promover transparência entre os provedores de internet que operam no Brasil, fortalecer a democracia e combater a disseminação de fake news e os discursos de ódio na internet.

O chamado Projeto de Lei das fake news visa a regulamentação das plataformas online, com o intuito principal de combater a propagação de desinformação e o uso de redes artificiais para

disseminar conteúdo falso, atribuindo uma série de obrigações as plataformas online (Henrique, 2023).

Caso se torne lei, o PL das fake news sugere o dever das plataformas gerenciar os assuntos compartilhados nas redes sociais, agindo antecipadamente com prevenção em relação aos conteúdos considerados “ilegais” e; divulgar na internet relatórios semestrais de clareza sobre a moderação dos conteúdo.

As plataformas serão responsabilizadas pelos assuntos impulsionados e monetizados, e deverão adotar medidas para impedir a disseminação de conteúdos ilegais, como atos de terrorismo, racismo, violência contra a mulher e crimes contra crianças e adolescentes. Também, será criado o Conselho de Transparência e Responsabilidade na Internet, composto por membros de diferentes setores da administração pública, responsável pelo acompanhamento das medidas estabelecidas, supervisionando os usuários da internet.

Em consequência da promoção da disseminação de fake news pode resultar em penas de um a três anos de prisão e pagamento de multas (Henrique, 2023).

Com isso, no artigo 3º, afirma que devem ser protegidos os fundamentos:

> a) a liberdade de expressão e de imprensa;
> b) a garantia dos direitos de personalidade, dignidade, honra e privacidade;
> c) o respeito à formação de preferências políticas e de uma visão de mundo pessoal do usuário;
> d) o compartilhamento da responsabilidade de preservação de uma esfera pública livre, plural, diversa e democrática;
> e) a garantia da confiabilidade e da integridade de sistemas informacionais;
> f) a promoção do acesso ao conhecimento de assuntos de interesse público;
> g) a proteção dos consumidores; e
> h) a transparência nas regras para anúncios e conteúdos patrocinados. (Coelho, 2020).

4 PANORAMA DOS CRIMES CIBERNÉTICOS NO BRASIL

A proposta deste capítulo, é apresentar que os crimes cibernéticos no Brasil apresentam um panorama desafiador, com uma variedade de ameaças em constante evolução.

4.1 Perfil do criminoso e das vítimas

Os perfis dos criminosos e das vítimas de crimes cibernéticos no Brasil podem variar bastante.

Mesmo que a evolução tecnológica está proporcionando facilidade para identificar algo ou pessoa em determinadas circunstâncias, existem ainda dificuldades persistentes para encontrar o agente que comete tal ato ilícito pelas redes sociais, o qual na maioria das vezes não são encontrados, em razão de não deixarem rastro e seu perfil não é único, podendo variar consideravelmente (Timóteo, 2017).

Os autores por práticas criminosas digitais podem apresentar um leque de perfis, devido a diversidade de comportamentos ilícitos que podem adotar. Diversos fatores são relevantes para analisar esses indivíduos, como motivação, idade, sexo, conhecimento técnico, recursos financeiros, organização e relação com a vítima (Reginald Junior, 2021).

Identificar um criminoso virtual não é tão fácil, pois não possui as mesmas características do criminoso clássico.

> Tatuagem, cor da pele, tamanho da cabeça, classe econômico-social já foram as características buscadas para identificar um criminoso. Hoje nem sequer podemos vê-lo, é uma ameaça invisível que vem atormentando os usuários da rede mundial de computadores (Brito, 2013, p.83).

Muitos dos criminosos possuem habilidades avançadas em informática, programação, redes e segurança cibernética, possuindo o conhecimento necessário para explorar os sistemas de computador e redes.

> É notório afirmar que os crimes virtuais mais elaborados são praticados por sujeitos com conhecimento aprofundado de informática, eletrônica e redes de computadores, esses indivíduos são denominados por hackers. Entretanto, o termo hacker não significa que o sujeito seja criminoso, muitos desses indivíduos utilizam-se do conhecimento e habilidades para o bem, como por exemplo, pode fazer parte do quadro de empregados em empresas ligada ao uso da internet e desenvolvem sistema de segurança informática (Fagundes, 2021).

O nome para tal criminoso pode ser visto como hacker que é usada para o agente que possui um grande conhecimento e habilidade em computação, porém ele trabalha de forma benéfica e legal. Porém, o cracker é o “hacker do mal”, na qual o seu foco é usar de suas

habilidades tecnológicas para causar prejuízos para outras pessoas, promovendo ações maléficas (Caetano, s.d.).

O perfil do criminoso pode variar de indivíduos autônomos a organizações criminosas mais complexas.

Alguns crimes cibernéticos são feitos por indivíduos, mas outros são realizados por grupos organizados, como gangues cibernéticas, hackers coletivos ou até mesmo organizações criminosas internacionais. Os criminosos cibernéticos frequentemente utilizam ferramentas especializadas, como kits de phishing, exploits de software, ransomware e malware personalizado, para realizar seus ataques.

Dentro do ambiente digital permite que os criminosos cibernéticos operem no anonimato, o que pode encorajar comportamentos criminosos cada vez mais. Além do mais, os criminosos digitais podem estar localizados em qualquer lugar do mundo, e estão evoluindo suas táticas para contornar medidas de segurança e explorar novas vulnerabilidades, tornando a proteção contra crimes cibernéticos um desafio em constante mudança (O que são crimes..., 2022).

> Com os avanços da inteligência artificial (IA), criminosos se passando por outras pessoas na internet se tornaram mais comuns do que se imagina, já que a perfeita execução de algumas ferramentas, como a *deepfake*, tecnologia que permite mudar o rosto em vídeo de maneira realista, tem aumentado os crimes cibernéticos (Nazar, 2023).
>
> No que concerne ao sujeito ativo dos crimes cibernéticos poderá ser qualquer pessoa, sendo classificado como crime comum, e quanto ao sujeito passivo considera-se qualquer pessoa que utilize ou não o meio eletrônico (Emanuely Costa, Raíla Silva, 2021).

As vítimas dos crimes cibernéticos no Brasil também têm uma variedade de perfis, isso inclui desde cidadãos comuns que podem cair em golpes de phishing ou ter seus dados pessoais comprometidos, até empresas de pequeno, médio e grande porte que podem sofrer ataques. Além disso, instituições governamentais e organizações sem fins lucrativos também podem ser alvos de ataques cibernéticos, visando roubar informações sensíveis ou interromper operações (Cosseti, 2020).

As vítimas dos crimes cibernéticos podem incluir indivíduos, instituições financeiras, governos e outros usuários de sistemas automatizados de informação, frequentemente conectados a terceiros. Assim, qualquer pessoa que utilize computadores ou a internet está suscetível a se tornar vítima de crimes cibernéticos, tanto pessoa física quanto jurídica (Reginald Junior, 2021).

Conforme dados do Ministério dos Direitos Humanos, estudos realizados pela Associação “SaferNet” em colaboração com o Ministério Público Federal, indicam que aproximadamente

366 crimes cibernéticos são reportados diariamente no Brasil, sendo as principais vítimas crianças e adolescentes (Nazar, 2023).

4.2 Casos famosos e tendências

Como antes referido, o incidente envolvendo a atriz Carolina Dieckmann, que deu origem a criação da lei 12.737/2012, na qual uma pessoa teve acesso as fotos intimas da atriz e acabou exigindo um dinheiro para que não divulgassem as fotos da atriz.

O incidente envolvendo Neymar Jr e a modelo Najila Trinade no ano de 2019, na qual Najila acusou o atleta de estupro. No decorrer da investigação, vídeos pessoais do jogador foram divulgados sem a sua permissão. O grande episódio gerou grande repercussão na mídia e nas redes sociais, levando os órgãos competentes a investigar possíveis delitos sob invasão de privacidade e divulgação não autorizada de imagens privadas/intimas. No desfecho, tanto Najila quanto seu ex-marido foram acusados pela Polícia Civil por fraude processual, extorsão e denunciação caluniosa (Martinelli, 2024).

Em razão da pesquisa CLearSale, durante o mês de dezembro de 2021, o aplicativo ConectSUS passou por uma interrupção de serviço, e foi informado que o conteúdo do portal do Ministério da Saúde, saude.gov.br, foi trocado por uma mensagem indicando que os dados internos dos sistemas foram copiados e removidos, totalizando 50 TB de informações nas mãos dos responsáveis. Logo após esse incidente, os perpetradores do ataque tornaram públicos códigos-fonte de estruturas pertencentes a órgãos do governo que foram obtidos durante a invasão ao Ministério da Saúde. Por meio de seu canal no Telegram, disponibilizaram para download um arquivo compactado com o nome "gitlab-app-saudegovbr.rar (Parte 1)", contendo 129 pastas repletas de ferramentas e códigos utilizados pelo governo em suas plataformas online, incluindo nomes de usuário, senhas e chaves de API. Além disso, o grupo responsável pelo vazamento também afirmou ter apagado uma quantidade significativa de dados presentes nos servidores governamentais, estimando em mais de 100 TB, porém ainda não há provas concretas que confirmem essa declaração (Ataques..., 2022).

No mês de março de 2022, a desenvolvedora de jogos Ubisoft declarou ter passado por um acontecimento de segurança virtual no começo do referido mês, ocasionando breves interrupções em certos jogos, sistemas e serviços oferecidos pela empresa. Certos usuários enfrentaram dificuldades ao tentar utilizar determinados serviços, além de plataformas de comercialização de jogos digitais e websites vinculados à corporação. As informações oficiais divulgadas pela Ubisoft apontam para um incidente interno, que aparentemente afetou apenas

os dados dos colaboradores, sem impacto direto nos consumidores. Diante disso, houve a suspensão temporária de alguns jogos, sistemas e serviços, com a necessidade de redefinição das credenciais de acesso dos funcionários como precaução. Apesar da situação, não foram divulgados indícios de exposição de dados internos, códigos-fonte ou documentos confidenciais, somente informações limitadas sobre a origem do incidente foram compartilhadas (Ataques..., 2022).

De acordo com a jornalista Tainá Falcão (2019), "o Brasil é o segundo pais com o maior número de crimes cibernéticos no mundo." Ou seja, o Brasil é um dos líderes mundiais em razão destes crimes.

Os incidentes de atividade delituosa envolvendo o uso de computadores como meio de ataque estão se expandindo rapidamente em escala global. No Brasil, as notificações de crime cibernético aumentaram em mais de 100% em 2018, conforme relatório da "SaferNet" (Brasil..., 2019).

No ano de 2022, foi realizado uma pesquisa através do Profissão Repórter, "os crimes virtuais no Brasil cresceram 175% durante a pandemia." (Crimes...2022).

> O Brasil registrou no primeiro semestre de 2022, 31,5 bilhões de tentativas de ataques cibernéticos a empresas. O número é 94% superior na comparação com o primeiro semestre do ano passado, quando foram 16,2 bilhões de registros. O Brasil é o 2º país na América Latina com mais ataques cibernéticos em 2022 (Oliveira, 2022; Pohlmann, 2023).

Somente entre janeiro e junho de 2021, o Brasil enfrentou mais de 16 bilhões de investidas de ataques cibernéticos, conforme apontado pelos dados coletados pelo FortiGuard Labs (Brasil..., 2021).

Uma pesquisa conduzida por uma empresa de cibersegurança revela que o Brasil ocupa a quarta posição global em termos de ataques via e-mail. Especialistas afirmam que o vazamento de dados e a crescente utilização de redes sociais incentivam os criminosos a adotarem métodos mais elaborados (Crime..., 2022).

Conforme Celso Freitas (2023), "o número de crimes na internet cresceu cerca de 5 % de 2021 para 2022, sendo em 2022 detectados mais de 120 milhões de arquivos com vírus espalhados pela rede em todo mundo."

4.3 Impactos na sociedade

Os crimes cibernéticos têm impactos significativos na sociedade em diversos níveis, isto é, representam uma ameaça complexa para a sociedade, com impactos que vão desde prejuízos financeiros até riscos à privacidade, segurança e estabilidade social, emocional e psicológico (Tocantins, 2024).

Consequentemente, é onde ficam visível os problemas, pois estes crimes resultam em prejuízos em diversas formas.

Nesse viés, conforme alega no site da Kaspersky que “tanto para indivíduos quanto para empresas, o impacto dos crimes cibernéticos pode ser profundo, acarretando principalmente danos financeiros, mas também perda de confiança e danos à reputação.” (O que são crimes..., 2022).

A invasão de sistemas e o roubo de informações pessoais representam uma ameaça à privacidade dos indivíduos, como dados bancários, de saúde e documentos pessoais, passiveis de exposição e uso inadequado.

Além do mais, vítimas de crimes cibernéticos muitas vezes experimentam estresse, ansiedade e medo em razão da violação de sua privacidade e segurança, na qual o psicológico é abalado, gerando um impacto gigantesco na saúde mental e no bem-estar emocional das pessoas afetadas.

As empresas e indivíduos podem sofrer danos referente à sua reputação como resultado das violações de dados ou incidentes de segurança cibernética, podendo afetar a confiança do público e a credibilidade das vítimas afetadas.

4.3.1 Principais setores críticos

No dizer da pesquisa Claranet, o Brasil lidera a lista de ameaças cibernéticas no campo da saúde, uma vez que suas médias são superiores aos números globais. A média brasileira registrou 1.613 incidências semanais de abril a setembro de 2022. Os criminosos estão interessados nos dados dos pacientes, como os tipos de tratamentos, números de benefícios, e informações de cartões de crédito ou de saúde, que são exploráveis para golpes e outros crimes. Esse tipo de ataque é especialmente danoso, pois muitos dados de saúde estão conectados a bases governamentais, como o SUS, onde a segurança cibernética é mais vulnerável devido à falta de investimento e maturidade comparado às empresas privadas. Para as empresas do setor, medidas essenciais incluem investir na prevenção de riscos, segmentar a infraestrutura e promover a conscientização sobre segurança digital. (Cibersegurança..., 2023).

O ramo da tecnologia está repleto de expectativas positivas de avanço com a introdução da conectividade 5G, que tem o potencial de transformar a transmissão de informações, principalmente em regiões mais distantes. No Brasil, esse setor está em franco crescimento, com vastas oportunidades ainda por explorar. Nos últimos 10 anos, houve um aumento estimado de 43% no número de empresas de tecnologia, um crescimento que foi impulsionado pela pandemia. Contudo, existem fragilidades nesse setor. Mesmo após a pandemia, a diminuição das demandas tecnológicas, aliada às pressões do cenário global, têm resultado em uma onda de demissões em grandes empresas. Essa situação leva as empresas a buscarem maior eficiência com menos recursos, o que implica em uma necessidade de mais responsabilidade e sagacidade nas decisões financeiras (Cibersegurança..., 2023).

Ademais, riscos ao setor de energia, na qual a matriz energética brasileira se destaca globalmente em termos de produção de energia limpa, com quase 50% de energia renovável em comparação com 15% globalmente. Olhando para a matriz energética, mais de 80% da energia elétrica é gerada a partir de fontes renováveis graças às hidrelétricas. Segundo a Agência Nacional de Energia Elétrica (Aneel), os riscos relacionados à cibersegurança incluem interrupções no fornecimento de energia, inviabilidade técnica operacional e perda de dados das empresas. A preocupação com o aumento dos crimes cibernéticos contra este cenário resultou a Aneel e o ONS (Operador Nacional do Sistema Elétrico) a criar uma rotina operacional de segurança cibernética para facilitar o amadurecimento do setor no Brasil. Este RO estabelece os padrões e controles mínimos que os agentes e operadores do Ambiente de Rede Regulado (ARCiber) devem adotar e implementar (Cibersegurança..., 2023).

Complementando, as ameaças ao ramo governamental que no segundo semestre de 2022, o número de ataques contra setores governamentais aumentou 95% a nível global. Principalmente de grupos de ransomware que atuam como atores do Estado-nação, destacando sequestros e apropriação indevida de dados. No Brasil, os ataques tiveram como alvo instituições e sites governamentais, em especial relacionados ao poder Judiciário. Muitas quantidades de informações confidenciais apresentam oportunidades lucrativas para os cibercriminosos conduzirem campanhas de phishing direcionadas, e as vulnerabilidades de violação de dados servem como um ponto de entrada fácil. Algumas das principais ameaças esperadas contra sistemas e serviços governamentais planejadas para 2023 incluem ataques de negação de serviço (DDoS), ransomware e hackers (Cibersegurança..., 2023).

5 PROCEDIMENTOS DE INVESTIGAÇÃO E MEDIDAS DE PREVENÇÃO DOS CRIMES CIBERNÉTICOS

No continente nacional, os procedimentos de investigação e medidas de prevenção dos crimes cibernéticos incluem a atuação de vários órgãos, as normas brasileiras Lei Carolina Dieckmann, o Marco Civil da Internet e a Lei Geral de Proteção de Dados, que ficam de frente aos crimes cibernéticos. Medidas de prevenção incluem educação e orientação digital, conscientização publica, uso de softwares de segurança e colaboração entre setores público e privado.

5.1 Desafios na Investigação

A investigação dos crimes cibernéticos no Brasil enfrenta uma série de desafios devido à natureza complexa dos delitos.

Em concordância com o ponto de vista de Renan Aguiar, Luis Neto, Maria Guida (2023), "a principal dificuldade na investigação desses crimes está na falta de evidências que comprovem a atividade criminosa em questão."

> Mesmo diante da constante evolução da tecnologia, as autoridades encontram dificuldades para investigar e solucionar os crimes virtuais, seja pela falta de legislação específica, seja pela carência de delegacias e profissionais especializados. Assim, a investigação acaba sendo lenta e complexa, o que gera a impunidade, pois, muitas vezes, ao identificar o autor de um crime, constata-se a ocorrência da prescrição. Isso facilita e explica o surgimento de vários novos golpes a cada dia (Lessa, Vieira, 2017, p.1).

Além do mais, apenas 17 dos 27 estados (incluindo DF) contam pelo menos com delegacia se tratando em crimes cibernéticos como: São Paulo, Bahia, Santa Catarina, Espírito Santo, Goiás, Maranhão, Minas Gerais, Mato Grosso, Rio de Janeiro, Sergipe, Distrito Federal, Pará, Tocantins, Paraná, Piauí, Pernambuco, Rio Grande do Sul (Delegacias..., s.d.).

Os criminosos cibernéticos constantemente utilizam técnicas avançadas para ocultar sua identidade, como o anonimato e serviços de mascaramento, impossibilitando a identificação e seu rastreamento.

> O anonimato desses criminosos está principalmente associado à Deep Web, que é uma parte da Internet usada para comunicações e trocas de arquivos de forma anônima, não indexada por mecanismos de busca convencionais. O acesso à Deep Web é possível por meio de aplicativos como a rede TOR (The Orion Route), que elimina os registros de acesso, embora alguns sites nessa rede possam exigir um login usando um

> navegador comum. Além disso, existe a Dark Web, uma pequena parte da Deep Web na qual os sites e redes também não são indexados por mecanismos de busca, mas diferem por serem voltados principalmente para atividades criminosas (Dorigon, Soares, 2018; Aguiar, Neto, Guida, 2023).

Aguiar, Neto e Guida (2023), concordam que "a quantidade de policiais capacitados e treinados na investigação de crimes virtuais que ainda é escassa, e por esse motivo passa a tornar-se um problema, pois resulta inevitavelmente na impunidade."

Pensamento de Spencer Sydow (2019), é que "não há um adequado preparo para as forças policiais, visto que se tem pessoas pouquíssimas qualificadas a atender a pessoa, receber, processar, investigar e periciar computadores."

Diante disso, a carência de profissionais qualificados nessas áreas pode ser um obstáculo para a eficácia das investigações, em que até mesmo os profissionais se veem despreparados para lidar com os delinquentes, que possuem uma especialização muito maior nesse tipo de delito (Junior, 2021).

> Seria um grande avanço se fosse elaborado um novo código especificando crimes virtuais, adentrando em todos seus aspectos e criando uma área policial especializada no assunto, com nível de conhecimento em computadores avançado para que possa se resolver o conflito de forma mais habilidosa, facilitando o encontro do criminoso virtual. Nota-se que o sistema jurídico não está totalmente preparado para coibir tais condutas, portanto se as normas que tratam de determinado assunto fossem, talvez, aperfeiçoadas, poderíamos ter a esperança de que os índices de criminalidade virtual reduziriam devido a eficácia de suas respectivas leis (Siqueira; et al., 2017, p.128).

5.1.2 Desafios no combate aos crimes cibernéticos

No pensar de Paulo Lima (2019), "a lei é extremamente lenta, com a tecnologia dando saltos e para mudar um artigo do Código Penal, demora se anos." Contudo, a legislação brasileira relacionada aos crimes cibernéticos nem sempre acompanha a evolução tecnológica e as novas formas de criminalidade digital, dificultando o combate aos cibercrimes.

Exemplificando, a lei 12737 "Carolina Dieckmann", representou um progresso significativo ao criminalizar a invasão de dispositivos eletrônicos para obter informações privadas. No entanto, não resolveu as questões legislativas vinculadas aos delitos virtuais, os quais têm apresentado um aumento constante (Andrade, 2021).

Afinal de contas, se trata de uma norma muito básica, contendo apenas quatro artigos, nas quais objetivam adulterar alguns artigos do Código Penal e de modo geral, ela tipifica um tipo de crime virtual e não em toda a sua dimensão, não expondo todos os tipos de crimes que há no

mundo virtual. Nesse sentido, a lei supracitada não tem tanta serventia na prática, sendo pouco efetiva, apesar de ser um marco (Cosseti, 2020).

Certamente, o Poder Legislativo deverá adquirir conhecimento sobre informática para conseguir detectar os problemas e, em seguida, criar legislações a respeito. Não é útil agir apenas quando os escândalos surgem, pois nesse momento as pessoas já sofreram prejuízos e não poderão mais ser protegidas pelo Estado (Sydow, 2019).

> De acordo com Wendt e Jorge (2021), a falta de capacitação de policiais, Ministério Público e Judiciário representa um desafio para combater o cibercrime, levando à impunidade. É crucial que esses profissionais sejam treinados continuamente por especialistas para acompanhar a evolução dos crimes cibernéticos (Aguiar, Neto, Guida, 2023).

O Brasil está atrasado em adotar medidas para combater os crimes cibernéticos, ocupando a 33ª posição em relação a segurança cibernética, em uma classificação que inclui 219 países (Cardoso, 2015).

Algumas estratégias e recursos que podem ser implementados para enfrentar os crimes cibernéticos são:

> ·Maiores especialistas em investigação e combate a crimes cibernéticos.
> ·A necessidade de investimentos em tecnologia e infraestrutura para apoiar as investigações.
> ·O estabelecimento de parcerias com empresas de tecnologia para aprimorar as técnicas de análise forense digital.
> ·A necessidade de atualização da legislação para abordar adequadamente os crimes cibernéticos.
> ·A importância de conscientizar a população sobre os riscos e as medidas de proteção no ambiente digital.
> ·O desenvolvimento de programas educacionais para ensinar habilidades digitais seguras desde a infância.
> ·A promoção de campanhas de conscientização sobre os impactos dos crimes cibernéticos e a importância de denunciá-los.
> ·A promoção de projetos de pesquisa e desenvolvimento de tecnologias avançadas para combater o cibercrime (Ludgero, 2023).

5.2 Como se proteger e denunciar os crimes cibernéticos

É essencial que as pessoas se previnam e se eduquem sobre o uso seguro da internet, utilizando com mais cautela e consciência.

Especificando, utilizar senhas fortes e complexas em diferentes contas, manter os softwares do sistema sempre atualizados para assegurar a segurança do computador, ter um antivírus ativo e fazer a remoção de ameaças regularmente, evitar clicar em links suspeitos e abrir anexos de origem desconhecida, nunca compartilhar informações pessoais para qualquer pessoa ou site, monitorar os extratos bancários atentamente para identificar atividades suspeitas, supervisionar

as atividades e afazeres online das crianças, se for realizar compras online preferir o cartão virtual, exercer um certo cuidado ao aceitar os termos de uso de sites e aplicativos, verificando se não há violação de privacidade, buscar por privacidade nas redes sociais restringindo quem pode ver as postagens; manter se atualizado sobre questões de segurança cibernética (Nóbrega, 2022; Cavalheiro, 2023).

Conforme o diretor de Educação e atendimento da SaferNet Rodrigo Nejm (s.d.), “o problema não está na tecnologia, mas, sim, no uso indevido da internet por parte das pessoas” (Zimmer, 2022).

Caso for vítima de um cibercrime, você pode fazer uma denúncia em qualquer delegacia próxima à sua residência, registrando um boletim de ocorrência ou buscar apoio em delegacias especializadas em crimes cibernéticos. Outro método de reportar uma denúncia é pela” SaferNet” Brasil que oferece um serviço para receber denúncias anônimas relacionadas a crimes cibernéticos, com procedimentos eficazes e transparentes para lidar com as denúncias recebidas pelo site (Cavalheiro, 2023; Machado, 2024).

É fundamental ter em mãos a maior quantidade possível de informações e provas do crime, como capturas de tela, comprovantes de transações bancárias e capturas de mensagens recebidas. Depois de reportar os delitos, é aconselhável que a vítima consulte um advogado especializado na área para obter orientação sobre os próximos procedimentos.

É importante destacar também que as vítimas também devem reforçar as medidas de segurança online (Crimes..., 2023).

6 CONCLUSÃO

Conforme foi exposto pela pesquisa, a internet é um meio importantíssimo para todos, revolucionando a forma como nos comunicamos, trabalhamos, aprendemos e nos entretemos e com isso a tendência é cada vez mais evoluir e evidentemente que virão novos crimes cibernéticos.

Diante da pesquisa, é claro que os crimes cibernéticos representam um desafio significativo para o jurídico brasileiro, exigindo medidas ágeis e eficazes por parte das autoridades e legisladores. As consequências jurídicas dos crimes cibernéticos no Brasil são múltiplas, abrangendo desde a necessidade de atualização legislativa até a capacidade de investigação

Respondendo à pergunta do começo da pesquisa: Como os desafios e dificuldades em combater e investigar os crimes cibernéticos no Brasil e suas poucas legislações levam a internet ser taxada de “terra sem lei” e como consequência leva a evolução e progresso cada vez mais?. Diante do estudo, a internet não pode ser considerada uma terra sem lei pois há alguns dispositivos e normas que ficam de frente aos crimes cibernéticos, porém é necessário evidenciar novas medidas eficazes por parte dos legisladores e um melhoramento no ordenamento jurídico. De forma geral, é importante que criem leis mais especificas e detalhadas com relação aos crimes cibernéticos, atendendo a grande complexidade e demanda que esses crimes possuem.

Complementando, ficou evidente que as investigações de crimes cibernéticos enfrentam dificuldades, então é importante profissionais mais especializados e preparados para o assunto e mais capacitação dos policiais que ficam de frente as investigações.

É primordial que, o Brasil avance no desenvolvimento de políticas públicas e estratégias de combate aos crimes cibernéticos, promovendo a cooperação entre todos. Além disso, é fundamental investir em educação digital e conscientização da população sobre os riscos, ameaças e consequências das atividades ilícitas na internet.

Concluindo, uma compreensão partindo de todos é essencial para a construção de um ambiente virtual mais seguro, onde os direitos dos cidadãos sejam protegidos e a justiça seja feita.

REFERÊNCIAS

A INTERNET, É uma terra sem lei? Saiba o que é o Marco Civil da Internet e as regulações que ele impõe. Advise blog, ano 2022. Disponível em: <https://blog.advise.com.br/a-internet-e-uma-terra-sem-lei-saiba-o-que-e-o-marco-civil-da-internet-e-as-regulacoes-que-ele-impoe/>. Acesso em: 15 fev 2024.

AGUIAR, Renan de Sousa; et al. **Crimes Cibernéticos: Analise do Processo Investigatório e os Desafios para combatê-los.** Revista ft, edição 127, (s.l.), ano 2023. Disponível em: <https://revistaft.com.br/crimes-ciberneticos-analise-do-processo-investigatorio-e-os-desafios-para-combate-los/>. Acesso em: 9 maio 2024.

ANDRADE, Sabrina. **Desafios no combate aos crimes cibernéticos - Redação Pronta**. Imaginie blog, (s.l.), ano 2021. Disponível em: <https://blog.imaginie.com.br/desafios-no-combate-aos-crimes-ciberneticos/>. Acesso em: 9 maio 2024.

ASSIS, Rebeka. **Crimes Virtuais: descubra quais são os 7 mais cometidos!** Jusbrasil, (s.l.), ano 2019. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-virtuais-descubra-quais-sao-os-7-mais-cometidos/784440112. Acesso em: 24 fev 2024.

ATAQUES, Cibernéticos: confira alguns casos famosos. Clearsale, (s.l.), ano 2022. Disponível em: <https://blogbr.clear.sale/ataques-ciberneticos-confira-alguns-casos-famosos>. Acesso em: 7 maio 2024.

BARBAGALO, Fernando Brandini. **O novo crime de fraude eletrônica e o princípio da legalidade.** Tribunal de Justiça, (s.l.), ano 2022. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade>. Acesso em: 25 mar 2024.

BARROS, Rodrigo Monteiro de. **Desafios Legais no Combate aos Crimes Cibernéticos: Uma Análise Jurídica.** Jusbrasil, (s.l.), ano 2024. Disponível em: https://www.jusbrasil.com.br/artigos/desafios-legais-no-combate-aos-crimes-ciberneticos-uma-analise-juridica/2181538097#:~:text=Fortalecer%20a%20legisla%C3%A7%C3%A3o%20nacional%20para,processos%20relacionados%20a%20crimes%20cibern%C3%A9ticos. Acesso em: 3 mar 2024.

BRASIL, É o segundo país com maior número de crimes cibernéticos. R7 Famosos e TV, (s.l.), ano 2019. Disponível em: <https://entretenimento.r7.com/famosos-e-tv/brasil-e-o-segundo-pais-com-maior-numero-de-crimes-ciberneticos-06102019/>. Acesso em: 21 abr 2024.

BRASIL, Pode aderir à Convenção de Budapeste sobre crimes cibernéticos. OpiceBlum, (s.l.), ano 2021. Disponível em: <https://opiceblum.com.br/brasil-pode-aderir-a-convencao-de-budapeste-sobre-crimes-ciberneticos/>. Acesso em: 25 abr 2024.

BRASIL, Sofre mais de 16,2 bilhões de tentativas de ataques cibernéticos. Redação, (s.l.), ano 2021. Disponível em: <https://securityleaders.com.br/brasil-sofre-mais-de-162-bilhoes-de-tentativas-de-ataques-

cibernetícos/#:~:text=Continua%20em%20crescimento%20o%20n%C3%BAmero>. Acesso em: 4 maio 2024.

BRASIL, É 2º em ranking de países que passam mais tempo em redes sociais. BBC News Brasil. Época Negócios, (s.l.), ano 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/09/brasil-e-2-em-ranking-de-paises-que-passam-mais-tempo-em-redes-sociais.html. Acesso em: 24 mar 2024.

BRASIL. Lei nº 12965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] República Federativa do Brasil.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 mar 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial [da] República Federativa do Brasil.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 mar 2024.

BRENOL, Marlise. **Perfil falso é crime? Saiba como identificar o golpe.** Serasa, (s.l.), ano 2023. Disponível em: https://www.serasa.com.br/premium/blog/perfil-fake-crime/. Acesso em: 3 mar 2024.

BRITO, Aurineu. **Direito penal informático**. 1º. ed. São Paulo: Saraiva, p.83, 2013. Acesso em: 1 mar 2024.

CABETTE, Eduardo Luiz Santos. **O novo crime de Invasão de Dispositivo Informático.** Consultor Jurídico, (s.l.), ano 2013. Disponível em: <https://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico/#author>. Acesso em: 24 mar 2024.

CAETANO, Érica. **O que é hacker?.** UOL, Brasil Escola. (s.l.), (s.d.). Disponível em: <https://brasilescola.uol.com.br/informatica/o-que-e-hacker.htm>. Acesso em: 5 abr 2024.

CARDOSO, Fabio Fettuccia. **Brasil está atrasado em estratégias de combate a crimes cibernéticos**. Jusbrasil, (s.l.), ano 2015. Disponível em: <https://www.jusbrasil.com.br/noticias/brasil-esta-atrasado-em-estrategias-de-combate-a-crimes-cibernetícos/180688777#:~:text=De%20acordo%20com%20dados%20do>. Acesso em: 6 maio 2024.

CAVALHEIRO, Renan. **Crimes cibernéticos: como se proteger?.** Academia de Forense Digital. (s.l.), ano 2023. Disponível em: <https://academiadeforensedigital.com.br/crimes-cibernetícos-como-se-proteger/>. Acesso em: 8 maio 2024.

CHAVES, Eduarda. **A LGPD no combate aos crimes cibernéticos.** Instagram, ano 2023. Disponível em: <https://www.instagram.com/p/CscAxruv3ka/?igsh=MTdub2Q5eXgzYWdrdA%3D%3D&img_index=1>. Acesso em: 10 mar 2024.

CIBERSEGURANÇA, :Veja os setores mais críticos no Brasil. Claranet, (s.l.), ano 2023. Disponível em: <https://www.claranet.com/br/blog/ciberseguranca-veja-os-setores-mais-criticos-no-brasil>. Acesso em: 9 maio 2024.

COELHO, Leonardo. **Lei das Fake News: o que é o PL 2630?** Politize, (s.l.), ano 2020. Disponível em: <https://www.politize.com.br/lei-das-fake-news/>. Acesso em: 21 maio 2024.

CONVENÇÃO, De Budapeste é promulgada no Brasil. Governo Brasil, (s.l.), ano 2023. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil>. Acesso em: 25 abr 2024.

CORDEIRO, Thomás. **Estelionato ganha força com internet, mas como evitar e denunciar?.** DDeL Associados, (s.l.), ano 2023. Disponível em: https://www.ddlassociados.com.br/estelionato-ganha-forca-com-internet-mas-como-evitar-e-denunciar/#:~:text=O%20que%20%C3%A9%20o%20estelionato,obtendo%20uma%20vantagem%20para%20si. Acesso em: 3 mar 2024.

COSSETI, Dickson. **Crimes Virtuais**. Série Debates, YouTube, (s.l.), ano 2020. Disponível em: <https://www.youtube.com/watch?v=LsHss6AGoAQ&t=558s>. Acesso em: 1 maio de 2024.

COSTA, Emanuely Silva; SILVA, Raíla Da Cunha. **Revista Eletrônica do Ministério Público do Estado do Piauí Crimes cibernéticos e investigação policial**. [s.l: s.n.], ano 2021. Disponível em: <https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf>. Acesso em: 8 abr 2024.

CRIME, Cibernético: Brasil é o 4º país do mundo com mais ataques por e-mail. Fala Brasil, R7, (s.l.), ano 2022. Disponível em: <https://record.r7.com/fala-brasil/videos/crime-cibernetico-brasil-e-o-4-pais-do-mundo-com-mais-ataques-por-e-mail-17112022/>. Acesso em: 4 maio 2024.

CRIMES, Cibernéticos: exemplos, o que diz a lei e como prevenir. Neon, (s.l.), ano 2023. Disponível em: <https://neon.com.br/aprenda/seguranca-digital/crimes-ciberneticos/>. Acesso em: 7 maio 2024.

CRIMES, Virtuais crescem no Brasil; veja flagrante e histórias de vítimas com o Profissão Repórter. Profissão Repórter, (s.l.), ano 2022. Disponível em: <https://g1.globo.com/profissao-reporter/noticia/2022/07/27/crimes-virtuais-crescem-no-brasil-veja-flagrante-e-historias-de-vitimas-com-o-profissao-reporter.ghtml>. Acesso em: 6 maio 2024.

D'URSO, Luiz Augusto Filizzola. **Advogado ensina como se proteger dos crimes virtuais**. TV Câmara São Paulo, ano 2019. Disponível em: <https://www.youtube.com/watch?v=yeNyMDIViKI&t=1s>. Acesso em: 8 maio 2024.

DELEGACIAS, Cibercrimes. Safernet, (s.l.), (s.d.). Disponível em: <https://new.safernet.org.br/content/delegacias-cibercrimes>. Acesso em: 11 abr 2024.

FACHINI, Tiago. **Lei Carolina Dieckmann: Tudo o que você precisa saber sobre.** Projuris, (s.l.) ano 2023. Disponível em: <https://www.projuris.com.br/blog/lei-carolina-dieckman-tudo-o-que-voce-precisa-saber-sobre/#:~:text=Perguntas%20frequentes->. Acesso em: 24 mar 2024.

FAGUNDES, Helenisse Nunes. **Crimes cibernéticos: é preciso conhecer para proteger-se.** Conteúdo Jurídico, (s.l.), ano 2021. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/56176/crimes-cibernticos-preciso-conhecer-para-proteger-se. Acesso em: 17 mar 2024.

FALCÃO, Tainá. **Crimes Cibernéticos.** Estúdio News, YouTube, ano 2019. Disponível em: https://www.youtube.com/watch?v=p2hk2ib_lhM. Acesso em: 25 abr 2024.

FREITAS, Celso. **Crimes cibernéticos: Brasil é um dos recordistas mundiais em arquivos com vírus na internet.** Jornal da Record, R7, (s.l.), ano 2023. Disponível em: <https://noticias.r7.com/jr-na-tv/videos/crimes-ciberneticos-brasil-e-um-dos-recordistas-mundiais-em-arquivos-com-virus-na-internet-13032023/>. Acesso em: 4 maio 2024.

HENRIQUE, Layane. **PL das Fake News: os 10 pontos principais para entender o projeto de lei | Politize!** Politize, (s.l.), ano 2023. Disponível em: <https://www.politize.com.br/pl-das-fake-news/>. Acesso em: 21 maio 2024.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016. Disponível em: https://archive.org/details/manual-de-crimes-informaticos-damasio-de-jesus-e-jose-antonio-milagre-2016/page/n71/mode/2up. Acesso em: 5 mar 2024.

JUNIOR, Reginald Vieira da Silva. **Os desafios do direito penal frente aos crimes cibernéticos.** Revista Científica Multidisciplinar Núcleo do Conhecimento, v. 03, n. 12, p. 121–143, 9 dez. 2021. Disponível em: https://www.nucleodoconhecimento.com.br/lei/crimes-ciberneticos. Acesso em: 27 abr 2024.

LEI, Carolina Dieckmann: 10 anos da lei que protege a privacidade dos brasileiros no ambiente virtual. Defensoria Pública, (s.l.), ano 2022. Disponível em: <https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/>. Acesso em: 24 mar 2024.

LESSA, Isabella Maria Baldissera; et al. **Crimes Virtuais: Análise do Processo Investigatório e Desafios enfrentados**. Simpósio, (s.l.), p.1, ano 2017. Disponível em: <https://egov.ufsc.br/portal/sites/default/files/594c13e45d209.pdf>. Acesso em: 9 maio 2024.

LIMA, Cláudio Vieira Guimarães. **Crimes Cibernéticos: O lado Obscuro da rede.** Goiânia, p.23, ano 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/2419/1/CL%c3%81UDIO%20VIEIRA%20GUIMAR%c3%83ES%20LIMA%20-%20TCC.pdf
CLÁUDIO VIEIRA GUIMARÃES LIMA - TCC.pdf (pucgoias.edu.br). Acesso em: 28 mar 2024.

LIMA, Paulo Marco Ferreira. **Crimes Cibernéticos.** Estúdio News, YouTube, ano 2019. Disponível em: https://www.youtube.com/watch?v=p2hk2ib_lhM. Acesso em: 25 abr 2024.

LUDGERO, Paulo Ricardo. **Desafios na Punição dos Cibercriminosos no Brasil: Estratégias para Combater a Impunidade.** Jusbrasil, (s.l.), ano 2023. Disponível em: https://www.jusbrasil.com.br/artigos/desafios-na-punicao-dos-cibercriminosos-no-brasil-estrategias-para-combater-a-impunidade/1862811103. Acesso em: 7 maio 2024.

MACHADO, Pureza. **Dia da Internet Segura: saiba como se proteger contra crimes cibernéticos.** YouTube, TV ALESE, ano 2024. Disponível em: <https://www.youtube.com/watch?v=MHu4syhPaaY&t=249s>. Acesso em: 8 maio 2024.

MACIEL, Rui. **Brasileiros são os que mais acreditam em fake news no mundo, diz pesquisa**. Canaltech, (s.l.), ano 2019. Disponível em: <https://canaltech.com.br/internet/brasileiros-sao-os-que-mais-acreditam-em-fake-news-no-mundo-diz-pesquisa-156387/#google_vignette>. Acesso em: 21 maio 2024.

MARTINELLI, Guilherme. **A Eficácia da Legislação Brasileira na Prevenção de Crimes Digitais.** Jusbrasil, (s.l.), ano 2024. Disponível em: https://www.jusbrasil.com.br/artigos/a-eficacia-da-legislacao-brasileira-na-prevencao-de-crimes-digitais/2147918640. Acesso em: 12 maio 2024.

MENDES, Paz. **Crimes Cibernéticos no Brasil: conheça os tipos, suas penas e agravantes.** Paz Mendes Sociedade de Advogados, (s.l.), ano 2021. Disponível em: https://www.pazmendes.com.br/crimes-ciberneticos-no-brasil/. Acesso em: 14 mar 2024.

MILAGRE, José Antônio. **O que muda com nova Lei que endurece e amplia pelas para crimes cibernéticos e virtuais? 14.155/2021**. YouTube, ano 2021. Disponível em: <https://www.youtube.com/watch?v=O_10gxcEHr0&t=1s>. Acesso em: 25 mar 2024.

MULLER, Nicolas. **O começo da internet no Brasil.** Oficina da Net, (s.l.), ano 2023. Disponível em: https://www.oficinadanet.com.br/artigo/904/o_comeco_da_internet_no_brasil. Acesso em: 28 jan 2024.

NAZAR, Susanna. **Casos de pedofilia virtual se multiplicam no Brasil com os avanços da inteligência artificial.** Jornal da USP, (s.l.), ano 2023. Disponível em: <https://jornal.usp.br/atualidades/casos-de-pedofilia-virtual-se-multiplicam-no-brasil-com-os-avancos-da-inteligencia-artificial/>. Acesso em: 6 abr 2024.

NERY, Carmen; BRITTO, Vinícius. **Internet já é acessível em 90,0% dos domicílios do país em 2021**. Agência IBGE Notícia, (s.l.), ano 2022. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021. Acesso em: 16 mar 2024.

NÓBREGA, Ana. **Como se proteger de crimes cibernéticos?.** ECycle, (s.l.), ano 2022. Disponível em: https://www.ecycle.com.br/crimes-ciberneticos/. Acesso em: 26 mar 2024.

O QUE É A LGPD?, Lei Geral de Proteção de Dados. Ministério Público, (s.d.), (s.l). Disponível em: <https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd>. Acesso em: 11 mar 2024.

O QUE SÃO CRIMES, Cibernéticos e como se proteger deles?. Kaspersky, (s.l.), ano 2022. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime>. Acesso em: 5 abr 2024.

O SENADO, E os crimes cibernéticos. Senado Federal, (s.l.), ano 2012. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/242982/EmPauta_235.pdf?sequence=6&isAllowed=y. Acesso em: 6 maio 2024.

OLIVEIRA, Ingrid. **Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%.** CNN Brasil, (s.l.), ano 2022. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/>. Acesso em: 3 maio 2024.

PERÍCIAS, Lopes. **Convenção de Budapeste para o Crime Cibernético e a importância da Computação Forense para o combate ao cibercrime no Brasil.** Jusbrasil, (s.l.), ano 2023. Disponível em: https://www.jusbrasil.com.br/artigos/convencao-de-budapeste-para-o-crime-cibernetico-e-a-importancia-da-computacao-forense-para-o-combate-ao-cibercrime-no-brasil/1810096919. Acesso em: 28 mar 2024.

PINHEIRO, Reginaldo César. **Os cybercrimes na esfera jurídica brasileira.** Jus Navigandi, (s.l.), ano 2000. Disponível em: https://jus.com.br/artigos/1830/os-cybercrimes-na-esfera-juridica-brasileira. Acesso em: 17 mar 2024.

POHLMANN, Otto. **Quais os grupos de hackers atuais mais perigosos do mundo?.** Terra, (s.l.), ano 2023. Disponivel em: https://www.terra.com.br/economia/quais-os-grupos-de-hackers-atuais-mais-perigosos-do-mundo,8614c761fd3d1d85ef3e8b44beb98276yzlxil5f.html. Acesso em: 3 maio 2024.

SAMARTINI, Frederico. **Qual a importância do Brasil ter aderido à Convenção de Budapeste contra crimes cibernéticos?.** JOVEM PAN NEWS, ano 2022. Disponível em: <https://www.youtube.com/watch?v=ChV_HT7w0cE&t=608s>. Acesso em: 25 abr 2024.

SCHWINGEL, Dino. **O que são crimes virtuais? Quais são os principais tipos de crimes digitais?.** YouTube, E-TRUST - Líder em Gestão de Identidades e Acessos. Ano 2020. Disponível em: <https://www.youtube.com/watch?v=UQtowtWWzz8&t=54s>. Acesso em: 10 mar 2024.

SENNA, Felipe; FERRARI, Daniella. **Convenção de Budapeste e crimes cibernéticos no Brasil - Migalhas**. Migalhas de Peso, (s.l.), ano 2020. Disponível em: <https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil>. Acesso em: 28 mar 2024.

SÉRVIO, Gabriel. **Metade da população mundial possui um smartphone, revela relatório.** Olhar Digital, (s.l.), ano 2021. Disponível em: https://olhardigital.com.br/2021/06/28/reviews/metade-da-populacao-possui-smartphone-revela-relatorio/. Acesso em: 16 mar 2024.

SIQUEIRA, Marcela Scheuer; et al. **Crimes Virtuais e a Legislação Brasileira Virtual Crimes and the Brazilian Legislation**. Pensando Direito, (s.l.), p. 128, ano 2017. Disponível em: <https://core.ac.uk/download/pdf/229767447.pdf>. Acesso em: 29 abr 2024.

STOFFEL, Simone. **O que são crimes virtuais? Quais são os principais tipos de crimes digitais?.** YouTube, E-TRUST - Líder em Gestão de Identidades e Acessos. Ano 2020. Disponível em: <https://www.youtube.com/watch?v=UQtowtWWzz8&t=54s>. Acesso em: 10 mar 2024.

SYDOW, Spencer Toth. **Crimes Cibernéticos.** Estúdio News, YouTube, ano 2019. Disponível em: https://www.youtube.com/watch?v=p2hk2ib_lhM. Acesso em: 25 abr 2024.

TIMÓTEO, Rafael. **STJ Cidadão #18 - Crimes Cibernéticos**. SUPERIOR TRIBUNAL DE JUSTIÇA (STJ), YouTube, ano 2017. Disponível em: <https://www.youtube.com/watch?v=or3mNrjTUxA&t=2s>. Acesso em: 26 abr 2024.

TOCANTINS, Hortencia Matos. **Crimes Cibernéticos na Atualidade: Desafio e Impactos na Sociedade.** Jus Brasil, (s.l.), ano 2024. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-na-atualidade-desafios-e-impactos-na-sociedade-moderna/2104354886. Acesso em: 5 maio 2024.

VIANA, Rodolfo. **O que é o Marco Civil da Internet? Desinformante explica.** You Tube, ano 2023. Disponível em: <https://www.youtube.com/watch?v=L0mKvO27n_g>. Acesso em: 28 mar 2024.

ZANOLINI, Lívia. **Crimes cibernéticos: quais são os principais e como se proteger.** Jovem Pan, (s.l.), ano 2021. Disponível em: <https://jovempan.com.br/programas/ta-explicado/crimes-ciberneticos-quais-sao-os-principais-e-como-se-proteger.html>. Acesso em: 10 mar 2024.

ZIMMER, Kelvin. **Veja 17 dicas simples para o uso consciente e seguro da internet.** Lumiun blog, (s.l.), ano 2022. Disponível em: <https://www.lumiun.com/blog/veja-dicas-simples-para-uso-consciente-seguro-da-internet/>. Acesso em: 8 maio 2024.