

UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

GLENDAYANE FELIX SANTOS

CIBERCRIMINALIDADE: o dilema da sociedade atual na utilização dos espaços virtuais

JUAZEIRO DO NORTE-CE
2023

GLENDAYANE FELIX SANTOS

CIBERCRIMINALIDADE: o dilema da sociedade atual na utilização dos espaços virtuais

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

Orientador: Prof. Francisco Gledson Lima Araújo.

JUAZEIRO DO NORTE-CE
2023

GLENDAYANE FELIX SANTOS

CIBERCRIMINALIDADE: o dilema da sociedade atual na utilização dos espaços virtuais

Este exemplar corresponde à redação final aprovada
do Trabalho de Conclusão de Curso de GLENDAYANE
FELIX SANTOS.

Data da Apresentação:

BANCA EXAMINADORA

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

Membro: PROF. ESP. ALYNE LEITE DE OLIVEIRA/ UNILEÃO

Membro: PROF. ESP. HUDSON JOSIMO VIANA / CENTEC

JUAZEIRO DO NORTE-CE
2023

CIBERCRIMINALIDADE: O DILEMA DA SOCIEDADE ATUAL NA UTILIZAÇÃO DOS ESPAÇOS VIRTUAIS

Glenda Slayane Felix Santos¹
Francisco Gledson Lima Araújo²

RESUMO

O artigo em questão aborda um dilema significativo enfrentado pela sociedade moderna: a distinção entre atividades legais e ilegais no ciberespaço. Este dilema é exacerbado pela crescente prevalência da cibercriminalidade, um fenômeno que inclui uma variedade de atividades ilegais realizadas através da internet. O estudo baseado na pesquisa bibliográfica, propõe-se a investigar a natureza da cibercriminalidade, examinando suas várias formas e a maneira como ela evoluiu com o tempo. Além disso, a pesquisa busca entender as leis e regulamentos existentes que governam a legalidade no ciberespaço, uma tarefa que se torna cada vez mais complexa à medida que a tecnologia avança a um ritmo acelerado. Também se propõe a avaliar o impacto da cibercriminalidade na sociedade. A justificativa para esta pesquisa reside na necessidade urgente de compreender melhor a cibercriminalidade. Este é um fenômeno que afeta indivíduos e organizações em todo o mundo, e a necessidade de proteger os usuários da internet nunca foi tão grande. Além disso, a distinção entre atividades legais e ilegais no ciberespaço é um dilema que precisa ser resolvido para manter a integridade do ciberespaço e garantir que ele continue sendo um espaço seguro para todos.

Palavras-Chave: Cibercriminalidade. Ciberespaço. Legalidade. Sociedade

ABSTRACT

The article in question addresses a significant dilemma faced by modern society: the distinction between legal and illegal activities in cyberspace. This dilemma is exacerbated by the growing prevalence of cybercrime, a phenomenon that includes a variety of illegal activities carried out over the internet. The study, based on bibliographic research, proposes to investigate the nature of cybercrime, examining its various forms and how it has evolved over time. In addition, the research seeks to understand the existing laws and regulations that govern legality in cyberspace, a task that becomes increasingly complex as technology advances at a rapid pace. It also proposes to assess the impact of cybercrime on society. The justification for this research lies in the urgent need to better understand cybercrime. This is a phenomenon that affects individuals and organizations around the world, and the need to protect internet users has never been greater. In addition, the distinction between legal and illegal activities in cyberspace is a dilemma that needs to be resolved to maintain the integrity of cyberspace and ensure that it continues to be a safe space for everyone.

Keywords: Cybercrime. Cyberspace. Legality. Society.

¹ Graduanda do Curso de Direito do Centro Universitário Doutor Leão Sampaio/Unileão. E-mail: glendaslayane003@gmail.com

² Professor Orientador. E-mail: gldaraujo@gmail.com

1. INTRODUÇÃO

A era digital, com seu advento no final do século XX e sua expansão acelerada no século XXI, trouxe consigo inúmeras conveniências e oportunidades. Transformou quase todos os aspectos da vida cotidiana, desde a maneira como as pessoas se comunicam até a maneira como trabalham, aprendem e se divertem. A internet, em particular, abriu um mundo de informações e possibilidades ao alcance de nossos dedos.

No entanto, como acontece com qualquer avanço tecnológico, essas oportunidades não vêm sem seus desafios. Um desses desafios, que tem se tornado cada vez mais prevalente na sociedade atual, é a cibercriminalidade. A cibercriminalidade abrange uma variedade de atividades ilegais realizadas através da internet, desde fraudes e roubos de identidade até ataques cibernéticos em grande escala que podem comprometer a segurança nacional.

Este fenômeno apresenta um dilema significativo para a sociedade: como distinguir entre atividades legais e ilegais no ciberespaço? Como é possível garantir que a lei seja aplicada de maneira justa e eficaz em um ambiente que é, por natureza, sem fronteiras e anonimato?

A problemática desta pesquisa reside precisamente neste dilema. Com a crescente prevalência da cibercriminalidade, torna-se cada vez mais importante para a sociedade entender e distinguir entre o que é legal e o que é ilegal no mundo virtual. Esta distinção não é apenas necessária para a aplicação eficaz da lei, mas também para a proteção dos usuários da internet. Afinal, todos nós temos o direito de navegar na web sem medo de sermos vítimas de atividades criminosas.

O objetivo geral desta pesquisa é analisar a natureza da cibercriminalidade e o dilema da sociedade atual em distinguir entre a legalidade e a ilegalidade no mundo virtual. Para alcançar este objetivo, a pesquisa se propõe a investigar a evolução da cibercriminalidade e suas várias formas, examinar as leis e regulamentos existentes que governam a legalidade no ciberespaço, e avaliar o impacto da cibercriminalidade na sociedade.

A justificativa para esta pesquisa reside na necessidade de compreender melhor a cibercriminalidade, um fenômeno que afeta indivíduos e organizações em todo o mundo. Além disso, a distinção entre atividades legais e ilegais no ciberespaço é um dilema que precisa ser resolvido para proteger os usuários da internet e manter a integridade do ciberespaço. Ao entender melhor a natureza da cibercriminalidade e as leis que a governam, podemos dar um passo importante para resolver esse dilema e criar um ciberespaço mais seguro para todos.

2. BREVE HISTÓRICO DA INTERNET

Para uma compreensão conceitual abrangente deste estudo, é indispensável uma análise contextual histórica sobre o surgimento da internet e sua relação com o direito brasileiro. Esta análise

servirá como base para a compreensão da cibercriminalidade, além de fornecer conceitos intrínsecos que auxiliarão no raciocínio.

Em sendo assim, a internet é uma extensa rede global que possui a capacidade de interconectar computadores em todo o mundo, possibilitando uma ampla troca de informações entre seus usuários. Isso é possível graças à sua vasta infraestrutura composta por software, hardware e protocolos de comunicação, que permitem essa conexão e comunicação entre dispositivos em todos os lugares (LEITE; LEMOS; 2014).

Para se chegar ao que atualmente se entende por internet, sob a perspectiva de um espaço virtual global, foram necessárias grandes inovações e a ocorrência de inúmeros fatores externos indispensáveis. A velocidade, conectividade, serviços e usabilidade que a internet possui atualmente são frutos das várias fases de sua evolução.

De acordo com Marcelo Xavier:

A Sociedade da Informação não surgiu repentinamente. Adveio de um longo processo de desenvolvimento, que, entendemos, num sentido amplíssimo pode ter o início vinculado à própria Revolução Industrial. Esta consistiu em um conjunto de mudanças tecnológicas com significativo reflexo na cadeia produtiva, seja em nível econômico, seja em nível social. Iniciada na Inglaterra ainda em meados do século XVIII, expandiu-se pelo mundo a partir do século XX (XAVIER, 2011, p.14)

Ainda conforme o autor, os avanços da tecnologia contribuíram para a formação da “sociedade da informação”, com a Revolução Industrial desempenhando um papel significativo e impactante em seu desenvolvimento. Destaca-se a substituição funcional da força humana pelo uso de máquinas. É notório que a inovação gradativa da era tecnológica trouxe diversas implicações benéficas para o desenvolvimento da humanidade. No entanto, essas transformações não apenas globalizaram e tecnologizaram a sociedade, mas também, como Sieber compreende, “tornaram-se fator de poder e de perigos potenciais”.

Partindo desse pressuposto, entende-se que a proporção que a internet, como tecnologia, tomou e vem constantemente ocupando na vida humana é imensurável. À medida que surgem seus benefícios, há espaço também para um impacto negativo. É o que se observa atualmente. De modo alarmante, diversas ações realizadas na internet não podem ser mensuradas ou controladas.

Nessa perspectiva, escreveram Casagrande, Costa e Fernandes (2015):

Cada vez mais acessíveis [...] com a tela touch screen, o toque com o dedo indicador confere poder a seu usuário. É um aparelho mágico capaz de transportar os espectadores da tela para lugares longínquos, sem que para isso seja preciso sair do lugar. Pequeno e portátil computador de mão, o celular permite uma comunicação multimodal, ajustado ao sistema de comunicação ubíquo, cuja fluidez suspende o tempo da reflexão. Tudo é feito de forma fluida, e se a usabilidade permite navegar no espaço de forma fácil pode pensar nos impactos psicossociais, financeiros, morais que os usuários da tecnologia sofrem por ser vítimas desses crimes, nos faz pretender buscar formas de ajuda-los, seja por meios legais de atuação do poder judiciário e legislativo ou meios sociais pelas políticas públicas ou programas sociais, portanto é indispensável entender e diagnosticar esses impactos (CASAGRANDE; COSTA; FERNANDES, 2015).

Portanto, *smartphones*, *tablets*, *computadores*, *smartwatch*, cada vez mais acessíveis, são ferramentas poderosas que permitem a comunicação multimodal³ e a exploração de espaços virtuais. No entanto, a facilidade de uso pode levar a impactos psicossociais, financeiros e morais, tornando essencial a compreensão e o diagnóstico desses efeitos. Ajudar as vítimas desses crimes através de meios legais e sociais é crucial para manter a integridade do ciberespaço.

2.1 A CIBERCRIMINALIDADE E SEUS ASPECTOS

É inegável que a internet proporcionou aos seus usuários um conhecimento e a transmissão de informações de forma rápida a qualquer hora e lugar, fatos que não ocorriam algumas décadas atrás, quando a comunicação à distância se dava por cartas, livros apenas impressos e notícias via jornais. À medida que a realidade humana é transformada pelas mudanças e evoluções digitais, vários fenômenos de transformação ocorrem e logo são externalizados no comportamento humano, pois internamente o ser humano e os seus comportamentos são moldados pelo externo.

Alinhado ao desenvolvimento tecnológico, percebe-se um necessário avanço mental e comportamental do homem no decurso do tempo, visto que de nada adianta uma máquina desenvolvida sem que haja um homem inteligente suficiente para dominá-la. Assim, com o progresso digital, nos dias atuais enfrentam-se desafios completamente diferentes de algumas décadas atrás, um claro exemplo são os crimes realizados no âmbito digital. A doutrina brasileira, embora ainda não tenha chegado a um denominador comum sobre a terminologia ideal a ser utilizada, refere-se a crimes digitais, cibercriminalidade ou computer crimes como uma ampla gama de atividades criminosas realizadas nos espaços virtuais (BARRETO, 2016.).

A doutrina oferece várias definições para o crime de informática. No entanto, optamos por formular e adotar a seguinte definição: “crime de informática é aquele que utiliza meios informáticos como ferramenta para alcançar o resultado desejado, bem como aquele cometido contra sistemas e meios informáticos”. Por meios informáticos, entendemos os hardwares e softwares de computadores, tablets, smartphones e outros dispositivos que podem ser usados para a prática criminosa (TEIXEIRA, 2022).

Os sujeitos ativos no âmbito criminal são aqueles que praticam alguma conduta legalmente delituosa (NUCCI, 2014). No contexto de crimes digitais, pode-se afirmar que o sujeito ativo é o próprio usuário da tecnologia da informação e comunicação que passa a utilizar de forma indevida e ilegal os meios digitais para cometer diferentes e incontáveis tipos de crimes. Em resumo, vale considerar que a expansão digital está inteiramente ligada à disseminação e facilidade no uso de

³ Diz-se da comunicação em que coexistem diversas modalidades comunicativas (fala, gestos, texto, processamento de imagem, etc.) <https://www.infopedia.pt/dicionarios/lingua-portuguesa/multimodal>, acessado em 30 de novembro de 2023.

tecnologias digitais em diversos aspectos da vida moderna. A adoção generalizada desses serviços criou raízes de tal forma que, nos dias atuais, raramente há quem não se utilize da tecnologia. Isso permitiu que a cibercriminalidade tenha um alcance maior de vítimas, visto que o campo para a prática desses atos vem constantemente se expandindo à medida que a tecnologia se desenvolve (JANAINE, 2022).

Os crimes digitais podem ser divididos em duas espécies conceituais do direito, crimes impróprios\impuros e próprios\puros. Dispondo sobre os crimes cibernéticos impróprios ou impuros, são aqueles em que o agente ativo se utiliza da tecnologia somente como um instrumento meio para a execução de crimes que já possuem uma tipificação penal e são praticados no mundo real, como exemplo se pode destacar os crimes de ameaças, contra a honra, furtos, extorsão. (BARRETO, 2016).

Em se tratando de crimes cibernéticos próprios ou puros, justamente o meio tecnológico é o alvo do sujeito, ou seja, a invasão de sistemas, a modificação de dados, o acesso a sistemas em sigilos, esse é o desejo do agente, o próprio sistema operacional é o alvo (BARRETO, 2016). Para melhor compreensão, pode-se observar o quadro abaixo:

Quadro 1 – Crimes Cibernéticos

CRIMES CIBERNÉTICOS	OS ATAQUES TÊM COMO ALVO	EXEMPLOS
Próprios / Puros	As estruturas dos sistemas informatizados	Invasão de dispositivos, danos aos sistemas informatizados, inserção de dados falsos em sistemas informatizados, etc.
Impróprios / Impuros	Bens jurídicos comuns, mas por meio cibernético	Extorsão, crimes contra honra praticados em redes sociais, furtos de valores em contas bancárias, lavagem de capitais, etc.

Fonte: Barreto (2016. P.17).

Portanto, a execução dos crimes digitais é considerada como crime meio, o que significa que a prática desses atos na internet é o meio utilizado para a realização de outras tipificações criminais. Por exemplo, no caso do estelionato, o sujeito ativo, por meio de artimanhas, ludibria virtualmente o sujeito passivo, levando-o ao erro para obtenção de uma vantagem econômica ilícita e, assim, causando prejuízo. A ação ocorre no ambiente virtual, mas o crime propriamente dito, não. Ressalta-se ainda que a internet surgiu inclusive como facilitadora, especificamente pelo fato de ajudar no

anonimato, pois a maior parte dos crimes cometidos no mundo virtual já existiam no mundo real, portanto a maioria dos conceitos são correlacionados ao do direito penal.

2.2 ASPECTOS TÉCNICOS DA CIBERCRIMINALIDADE

Os crimes cibernéticos envolvem uma diversidade de aspectos técnicos, uma vez que são perpetrados no ambiente digital. Os cibercriminosos aproveitam-se das tecnologias da informação e das vastas funcionalidades que são oferecidas a seu favor, levando em consideração que a internet possibilita o cometimento de crimes sem limites territoriais, permitindo um alcance de vítimas e diferentes tipos de ataques ao mesmo tempo (UPIS, 2019).

Para melhor percepção de quais formas os criminosos atuam, citam-se alguns dos principais aspectos técnicos dos crimes digitais:

Hacking - os hackers utilizam seus conhecimentos e habilidades técnicas para obter acessos indevidos e não autorizados a sistemas de computador, redes ou dispositivos e, com isso, corrompem o sistema. Tal ação pode ser possível através da exploração de vulnerabilidades, uso de malware ou inclusive a força bruta para adivinhar senhas (TEIXEIRA, 2022).

Malware é uma categoria extensa que engloba software malicioso, como vírus, trojans, *spyware* e *ransomware*. Esses programas são projetados justamente para infectar sistemas e causar danos, bem como roubar informações ou extorquir dinheiro (TEIXEIRA, 2022).

O *phishing* é uma técnica utilizada em que os criminosos enviam mensagens por um e-mail falso ou websites fraudulentos que se assemelham a comunicações verdadeiras, sendo capazes de ludibriar as vítimas para revelar informações confidenciais, como senhas ou informações pessoais financeiras (TEIXEIRA, 2022).

A engenharia social se refere à manipulação psicológica das pessoas com o intuito de obter informações confidenciais. Tal manipulação envolve a persuasão de alguém a revelar senhas ou outras informações confidenciais por meio de interações pessoais ou telefônicas. Todos os aspectos técnicos citados acima e as dezenas de formas utilizadas tanto na *Deep Web* quanto na *Dark Web* deixam um enorme sinal de alerta a todos os envolvidos quanto à sua segurança (TEIXEIRA, 2022).

A *Deep Web* e a *Dark Web* são partes distintas da internet que não são acessíveis por meio de mecanismos de busca padrão. A *Deep Web* refere-se a todas as páginas da web que não estão indexadas pelos mecanismos de busca, incluindo bancos de dados, fóruns privados, registros médicos e páginas de pagamento seguras. Por outro lado, a *Dark Web* é uma pequena parte da *Deep Web* que foram intencionalmente ocultadas e é inacessível por meio de navegadores web padrão. É frequentemente associada a atividades ilegais, como tráfico de drogas, cibercrime e serviços ilícitos,

embora também seja usada para atividades legítimas, como ativismo político e jornalismo em regiões onde a liberdade de expressão é limitada (CALDERON, 2017).

A *Dark Web* é frequentemente vista como um espaço sem regras, onde uma variedade de atividades ilegais pode ocorrer com relativa impunidade. Este ambiente, marcado pelo uso de criptografia e pelo anonimato de seus usuários, tem se tornado um terreno fértil para a prática de crimes cibernéticos. A facilidade com que informações podem ser trocadas na internet e como isso pode colocar a privacidade, intimidade e segurança das pessoas em risco, se tornou um grande problema dentro da seara jurídica (CALDERON, 2017).

A proliferação de práticas ilegais e criminosas na *Dark Web* é um problema crescente. A legislação atual não é suficientemente efetiva para coibir a atuação desses criminosos. À medida que a sociedade continua convivendo com o crescimento tecnológico, são necessárias legislações que protejam os usuários e delimitem até onde esses avanços podem evoluir (CALDERON, 2017).

No entanto, a *Dark Web* também apresenta desafios significativos para a aplicação da lei. A natureza anônima e criptografada da *Dark Web* torna difícil rastrear e identificar os perpetradores de crimes cibernéticos. Além disso, a falta de uma legislação brasileira específica para a proteção dos usuários de “coisas” conectadas à internet cria uma oportunidade para a criação de novas leis. Assim, a *Dark Web* continua a ser um espaço complexo e desafiador para a aplicação da lei e a proteção dos usuários da internet (CALDERON, 2017).

Compreender alguns dos aspectos técnicos ligados aos crimes digitais é fundamental para prevenir, detectar e responder a inúmeras ameaças cibernéticas às quais os usuários estão à mercê. À medida que a tecnologia evolui, os criminosos digitais também desenvolvem novas técnicas e táticas, tornando indispensável uma abordagem contínua e adaptativa para a segurança cibernética. A abordagem deve ser tanto técnica quanto pedagógica, com medidas que permitam uma navegação mais segura, e também legislativa, apesar de existir algumas leis, dentre elas o Marco Civil da Internet e a Lei Carolina Dickmann, estas foram criadas certamente em um momento que os crimes não tinham tanto amplitude e complexidade, contudo espera-se a proposição de leis que assegurem que os crimes eventualmente cometidos através das modalidades informáticas sejam coibidos de forma exemplar.

2.3 O CRIME DE GOLPES FINANCEIROS PELA INTERNET

A internet tem um impacto significativo nas operações econômico-financeiras, sendo o comércio eletrônico um exemplo notável. Este não é apenas realizado por empresas nascidas no ciberespaço, conhecidas como empresas pontocom, mas também por empresas tradicionais que se adaptaram à realidade atual para aproveitar a tecnologia e evitar a perda de mercado e a falência. Isso

pode ser devido à ineficiência em relação às empresas tecnologicamente avançadas ou à falta de aproveitamento das oportunidades de negócios à distância, expandindo seus horizontes (BRITO, 2013)

As fraudes perpetradas no ambiente virtual impactam os usuários das mais variadas formas, tais como: a fraude em transferências, compras e pagamentos através de links falsos e investimentos e em organizações fraudulentas, investimentos em moedas virtuais, e jogos ilegais hospedados em sites fora do Brasil, um bom exemplo tem sido o jogo Fortune Tiger (jogo do tigre) que levou muitos usuários a perder valores enormes em apostas, levando inclusive a investigação da Polícia Civil do Maranhão, que apreendeu bens ligados à influenciadora digital Skarlete Mello que divulgava em suas redes sociais, levando vários usuários a apostarem e perderem seus valores (G1, 2023).

Portanto, os usuários de internet estão a mercê da cibercriminalidade na medida que estes na sua falta de informação e na ânsia de lucro rápido são levados a erro por grupos criminosos especializados em crimes na rede mundial de computadores.

2.4 CRIME DE VAZAMENTO DE DADOS

O vazamento de dados é uma das maiores ameaças à segurança digital na era moderna. Com o aumento da digitalização, a quantidade de dados pessoais e corporativos disponíveis online cresceu exponencialmente. Infelizmente, isso também aumentou a incidência de crimes de vazamento de dados.

O vazamento de dados ocorre quando informações confidenciais são liberadas ilegalmente para um ambiente não seguro. Isso pode acontecer de várias maneiras, incluindo ataques cibernéticos, negligência interna e falhas de segurança. Os dados vazados podem incluir informações pessoais identificáveis, como nomes, endereços e números de segurança social, bem como dados corporativos sensíveis.

Os efeitos de um vazamento de dados podem ser devastadores. Para indivíduos, pode resultar em roubo de identidade e fraude financeira. Para empresas, pode levar a perdas financeiras significativas, danos à reputação e perda de confiança do cliente.

A legislação em muitos países considera o vazamento de dados um crime, o Brasil está incluído nesse rol. Por exemplo, no Brasil, a Lei Geral de Proteção de Dados (LGPD) 13.709/18, criada recentemente justamente por entender que os dados são ativos importantes, inclusive com a Emenda Constitucional nº 115, datada de 10 de fevereiro de 2022, que alterou a Constituição Federal para considerar a proteção de dados pessoais como parte dos direitos e garantias fundamentais. A Lei 13.709/18 estabelece regras estritas sobre o uso e a proteção de dados pessoais e prevê penalidades severas para violações, penalidades estas que vão desde multas que podem variar entre 2% do

faturamento bruto e até 50 milhões de reais, bloqueio total do uso do banco de dados dos clientes pela empresa (PECK, 2021).

No entanto, apesar das leis existentes, o crime de vazamento de dados continua a ser um problema significativo. Isso se deve em parte à natureza global da internet, que torna difícil rastrear e processar os criminosos. Além disso, muitas empresas ainda não implementaram medidas de segurança adequadas para proteger seus dados.

Para combater o crime de vazamento de dados, é essencial que tanto indivíduos quanto empresas tomem medidas para proteger seus dados. Isso inclui o uso de senhas fortes, a habilitação de autenticação de dois fatores e a manutenção de softwares e sistemas atualizados. Além disso, as empresas devem investir em treinamento de segurança cibernética para seus funcionários e considerar a contratação de profissionais de segurança cibernética (TEIXEIRA, 2022).

Em resumo, o crime de vazamento de dados é uma ameaça séria na era digital. É essencial que sejam tomadas medidas para proteger os dados e pressionando para que as leis no caso a LGPD seja mais fortemente aplicada e naturalmente a fiscalização seja mais rigorosa para combater esse crime.

2.5 DOS DELITOS INFORMÁTICOS CONTRA A CRIANÇA E O ADOLESCENTE

O crescimento dos crimes contra crianças e adolescentes envolvendo a internet tornou-se uma questão de preocupação global. Apesar da existência do Decreto n. 99.710/90, que ratificou a Convenção sobre os Direitos da Criança, e do Decreto n. 5.007/2004, que ratificou o protocolo opcional a essa Convenção, as práticas que exploram a vulnerabilidade física e mental dessas vítimas continuam aumentando em todo o país (BRITO, 2013).

A Constituição da República Federativa do Brasil, no seu art. 227, dispõe sobre a linha de tratamento dispensado às Crianças e aos Adolescentes:

Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

(...)

§ 4º – A lei punirá severamente o abuso, a violência e a exploração sexual da criança e do adolescente.

Em conformidade com os princípios constitucionais, o Estatuto da Criança e do Adolescente (ECA) - Lei n. 8.069/90 - no seu artigo 1º, institui o Princípio da Proteção Integral para crianças (indivíduos com menos de doze anos) e adolescentes (indivíduos entre doze e dezoito anos). O artigo 5º do mesmo estatuto estabelece que esses indivíduos não devem ser submetidos a qualquer forma de

negligência, discriminação, exploração, violência, crueldade ou opressão. Qualquer violação desses direitos fundamentais, seja por ação ou omissão, será punida de acordo com a lei (BRITO, 2013).

Diariamente a mídia relata muitos casos de abuso sexual no ambiente digital por cibercriminosos, envolvendo crianças e adolescentes. Por um lado, é inegável que a internet facilitou a expansão e ação de pedófilos, que se aproveitam do anonimato proporcionado pela rede. Por outro lado, a mesma internet pode ser usada como uma ferramenta eficaz no combate à pedofilia e à pornografia infantil.

Além de ferramentas que possibilitam o rastreamento de suspeitos, a internet facilitou a criação de um centro unificado para denúncias de pedofilia praticada online. Este centro é o resultado de um acordo entre a Secretaria Especial de Direitos Humanos, a Polícia Federal e a ONG SaferNet. Ele permite que a Polícia Federal tenha acesso imediato ao banco de dados para investigar informações sobre os crimes, acelerando o início das investigações e a remoção de páginas inadequadas da internet. O centro também serve para alimentar a base de dados do governo federal, ajudando a identificar onde ocorrem mais delitos, se as vítimas são crianças brasileiras e, assim, direcionar a formulação de políticas públicas de combate à pedofilia. (BRITO, 2013).

Quando a tecnologia avançada é usada para cometer crimes, muitas vezes ela se mantém à frente das leis penais. Isso pode prejudicar o trabalho dos profissionais envolvidos na perseguição criminal, pois eles encontram limitações legais.

2.6 APLICAÇÃO DA LEI PENAL NO CIBERESPAÇO

O termo “ciberespaço” refere-se a um espaço virtual, não físico, formado pela interconexão global de redes de computadores. Representa um ambiente digital onde as interações ocorrem por meio de dispositivos eletrônicos e redes de comunicação, como a internet. O conceito foi popularizado pelo autor de ficção científica William Gibson em seu livro “*Neuromancer*”, publicado em 1984. O ciberespaço não possui uma localização física tangível; em vez disso, é um espaço eletrônico que transcende fronteiras geográficas.

Nesse ambiente, as pessoas podem se comunicar, compartilhar informações, realizar transações, criar conteúdo digital, entre outras atividades. A diferença entre o espaço virtual e físico não se dá apenas pelos aspectos topográficos, mas também pela fluidez em suas estruturas virtuais e a rigidez do espaço físico. À medida que cada um tem suas características específicas, ambos os espaços não se excluem, mas se complementam, conforme entende o filósofo Pierre Lévy.

A aplicação da lei no ciberespaço apresenta diversos e significativos desafios para os países em todo o mundo. Esses desafios surgem devido à natureza global, dinâmica e descentralizada da internet. Reflexões sobre os espaços virtuais levam à afirmação de que este se trata de um “não

espaço”, dificultando ainda mais a aplicação da lei penal, levantando a questão: como aplicar uma pena a alguém que cometeu o crime em um “não espaço”? No entanto, não importa onde seja, em algum local o crime praticado na internet produzirá o seu resultado no mundo real (ZACARRIAS; 2004).

A rápida evolução da tecnologia no ciberespaço muitas vezes ultrapassa a capacidade dos sistemas legais e regulatórios de se adaptarem. Isso cria lacunas nas leis e nas práticas de aplicação, pois a internet transcende fronteiras nacionais, tornando um grande desafio determinar qual jurisdição deve aplicar a lei em casos específicos. Crimes cibernéticos podem ser cometidos de um país para outro, dificultando a cooperação entre autoridades (ZACARRIAS; 2004).

Nesse sentido, a falta de padrões internacionais claros para regulamentar o comportamento online dificulta a criação de legislação eficaz e a cooperação entre diferentes jurisdições. Para enfrentar os desafios advindos da aplicação e identificação da lei penal no espaço, é indispensável que os países trabalhem conjuntamente para desenvolver leis e normas internacionais, além de fortalecer a cooperação internacional entre agências de aplicação da lei (ROSSINI; 2004).

A criação de acordos e tratados bilaterais ou multilaterais pode auxiliar a estabelecer uma base legal para abordar questões específicas no ciberespaço. Ademais, o desenvolvimento de capacidades técnicas e treinamento adequado para profissionais da área jurídica e de segurança cibernética é crucial para lidar com os problemas em constante evolução.

O Brasil levou um tempo considerável para se tornar signatário da Convenção de Budapeste do Conselho Europeu sobre Cibercrime, acontecendo apenas através do Decreto nº 11.491, de 12 de abril de 2023. O documento do Conselho Europeu reflete a preocupação mundial com este tipo de crime e enfatiza que um problema dessa magnitude deve ser enfrentado de maneira global e uniforme. Ainda recomenda que os Estados atualizem suas legislações de acordo com as diretrizes contidas na convenção.

Além da inclusão da Convenção de Budapeste ao nosso ordenamento, como citado anteriormente o Brasil tem o Marco Civil da Internet, também conhecido como Lei nº 12.965 de 2014, é uma legislação que regula o uso da internet no Brasil. Esta lei foi criada com o objetivo de estabelecer direitos, garantias e deveres no uso da internet.(TEIXEIRA, 2023)

Um aspecto importante é a proteção da privacidade. A lei protege a privacidade dos usuários da internet, garantindo que suas informações pessoais não sejam coletadas ou usadas sem o seu consentimento.

A lei 12.965/14 também estabelece a responsabilidade dos agentes de acordo com suas atividades. Isso significa que as empresas e indivíduos que operam na internet são responsáveis por suas ações e podem ser responsabilizados por violações da lei (TEIXEIRA, 2013).

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Em resumo, o Marco Civil da Internet é uma legislação importante que protege os direitos dos usuários da internet no Brasil, promove a liberdade de expressão e a privacidade, e estabelece regras claras para o uso responsável e ético da internet para todos os agentes envolvidos, sejam eles usuários ou provedores.

Outra lei de relevante importância no combate aos crimes cibernéticos é a lei Carolina Dickmann, que originou-se do Projeto de Lei 2793/2011, apresentado pelo deputado Paulo Teixeira (PT-SP), e tramitou em regime de urgência no Congresso Nacional, entrando em vigor em tempo recorde se comparado com outros projetos também sobre delitos informáticos.

Foram aprovados os Projetos de Lei n. 35/2012 que foram inicialmente originados pelo Projeto de Lei n. 2.793/2011, no qual houve uma proposta modificativa do Projeto de Lei n. 84/99 (Lei Azevedo), sendo certificada e publicada pela Lei 12.737/12 com o objetivo de combater a ocorrência de crimes cibernéticos.

Ela ganhou notoriedade e o nome de Lei Carolina Dieckmann em virtude da repercussão do caso no qual a atriz teve o seu computador pessoal invadido e seus arquivos pessoais roubados, causando a publicação de fotos íntimas suas na internet, por meio das redes sociais. Devido ao alarde que esta situação causou, a lei foi um importante instrumento para punição dos crimes virtuais.

Essa lei trouxe em seu bojo, a possibilidade da aplicação de sanção, nas condutas de violação de dados, estabelecendo a tipificação criminal de delitos informáticos, Incluindo ao Código Penal os artigos 154-A e 154-B, o legislador autorizou a punição daquele infrator que, com a vontade de cometer a conduta delitiva, sem consentimento da vítima, invade dispositivo informático, com a intenção de obter, destruir ou alterar informações pessoais que estejam no dispositivo (PECK, 2021).

Os usuários de internet tem leis que protegem a sua navegação, contudo resta saber se estas são suficientes, uma vez que de acordo com reportagens diárias, é cada vez mais frequente notícias de vazamentos de dados, perfis fakes, fraudes financeiras, vazamentos de dados entre outros. É necessários então uma abordagem ampla envolvendo educação no bom uso da rede mundial de computadores alertando sobre privacidade, crimes e o bom uso, como também o combate mais rigoroso aos criminosos.

3 METODOLOGIA

A pesquisa realizada possui natureza da pesquisa é básica, um tipo de investigação que tem como objetivo resolver um problema prático ou desenvolver uma solução para uma necessidade específica. Essa abordagem se concentra na aplicação prática do conhecimento adquirido por meio dos estudos. Portanto, ao final desta pesquisa, será possível auxiliar os usuários da internet a identificar, quando possível, que estão sendo vítimas de crimes cibernéticos e a se prevenir desses.

Quanto aos objetivos, a pesquisa é descritiva, com o propósito de descrever e analisar as características de uma população, fenômeno ou evento. Trata-se de uma abordagem que se concentra na observação sistemática e na coleta de dados sobre o que está acontecendo, sem interferir ou manipular o ambiente. Dessa forma, esta pesquisa buscou entender, caracterizar e descrever os aspectos da cibercriminalidade, tais como: compreender as características das vítimas e do sujeito ativo dos crimes digitais, as frequências com que eles ocorrem, e os impactos na vida do sujeito passivo.

Em relação às fontes, a pesquisa é bibliográfica, que é uma das principais fontes que fornecem conhecimentos e informações utilizadas em pesquisas de várias áreas do conhecimento. Ela pode ser definida como o material que fornece informações com base sólida sobre um determinado tema ou objeto de estudo, como documentos escritos, fotografias, artigos científicos, entre outros, para que se possa chegar a uma compreensão do que se pretende.

4 RESULTADOS OBTIDOS

Ao longo deste trabalho, pode-se observar que a internet modificou amplamente a vida humana, em termos de inteligência, agilidade e comunicação. Inúmeros foram os benefícios advindos dessas transformações. No entanto, alguns pontos negativos também surgiram, impactando fortemente o comportamento humano e fomentando o aumento de crimes. A princípio, a partir do momento em que o homem percebe diante de si uma facilidade em se beneficiar ilicitamente e causar danos a outrem sem ao menos sair de casa e com uma imensa facilidade de anonimato, novos desafios surgem.

Nesse sentido, compreendeu-se que embora a disponibilidade de acesso a informações sem restrições seja um fator contributivo para o progressivo aumento de crimes cibernéticos, essa não é a única causa que leva um sujeito ativo ao cometimento dessas modalidades criminosas. São vários os fatores que abrem espaços para esses atos, tendo em vista que esses elementos não surgem isoladamente, mas diante das suas condições se completam.

Portanto, concluiu-se que a disponibilidade de acesso a informações sem restrições, associada a vulnerabilidades dos sistemas, as técnicas cada vez mais aprimoradas dos sujeitos ativos e a falta

de lei eficaz para punir os infratores, são as principais causas que levam ao aumento da cibercriminalidade. Ao desenvolver a pesquisa, descobriu-se que tanto os sujeitos ativos quanto os passivos da cibercriminalidade possuem atributos particulares passíveis de destaque.

Alguns tipos de crimes realizados no âmbito digital, como golpes financeiros, o agente se passa por alguém, seja através do *hackeamento* de conta ou até mesmo como estelionatário, para obter vantagem financeira ilícita. Seu principal desejo nesse caso é apenas obter para si ou para outrem vantagem pecuniária. Um cenário como este tem ocorrido diariamente, e embora já estejam aprimorando suas técnicas capazes de enganar alguém, tem sido cada vez mais fácil identificá-los. Através da análise de alguns relatos reais de quem teve sua conta hackeada, foi possível perceber que nessa modalidade, vários pontos em comum se encontram.

Por exemplo, Yngrid da Silva Paixão teve seu Instagram hackeado em 11/09/2022 e algumas postagens foram feitas em seu nome. Julio Cesar Belém teve seu Instagram hackeado em 31/10/2023 e postagens foram feitas em seu nome. Laura Fernandes teve postagens feitas em seu nome em 15/11/2023.

Nestes exemplos reais que ocorrem constantemente, embora os criminosos não tenham utilizado as mesmas palavras, seus objetivos seguem a mesma direção. Eles induzem alguém a acreditar que, com apenas alguns centavos ou poucos reais, se beneficiará com automóveis ou grandes quantias de dinheiro. Em outras palavras, eles se apropriam do Instagram de um usuário e, a partir de postagens direcionadas, fazem com que os seguidores acreditem que são reais e acabam transferindo valores ou tendo suas contas bancárias bloqueadas.

Com suas habilidades técnicas em engenharia social, *phishing*, exploração de vulnerabilidades ou uso de malware, associadas à motivação financeira e à facilidade no anonimato e camuflagem com o uso de redes privadas virtuais (VPNs) ou servidores proxy, esta é apenas uma das inúmeras formas utilizadas para obter esse tipo de vantagem econômica.

A internet tornou-se um ambiente inseguro, tornando-se indispensável que os usuários adotem boas práticas de segurança digital, atentando-se para os perigos e ameaças potenciais. Por vezes, precauções simples como: ativar a autenticação de dois fatores para adicionar uma camada extra de proteção, atualizar o software, pois as atualizações geralmente corrigem as vulnerabilidades dos sistemas; não clicar em links suspeitos ou compartilhar informações pessoais com fontes não confiáveis, ou até configurar uma senha forte para a rede Wi-Fi e usar protocolos de segurança, como o WPA3, podem ajudar a evitar o acesso não autorizado à sua rede.

O objetivo inicial específico deste trabalho, além de refletir a urgente necessidade de fortalecimento de ações preventivas e repressivas no combate a crimes cibernéticos, foi diagnosticar os maiores impactos e consequências na vida dos sujeitos passivos. Nesse ponto, percebeu-se que os principais impactos estão relacionados a perdas financeiras, devido a fraudes bancárias, roubo de

identidade, atividades fraudulentas ou compras não autorizadas que afetam as contas bancárias, e impactos psicológicos e emocionais associados ao estresse, ansiedade e angústia emocional devido à invasão da privacidade, a sensação de vulnerabilidade e preocupações com a duração do crime.

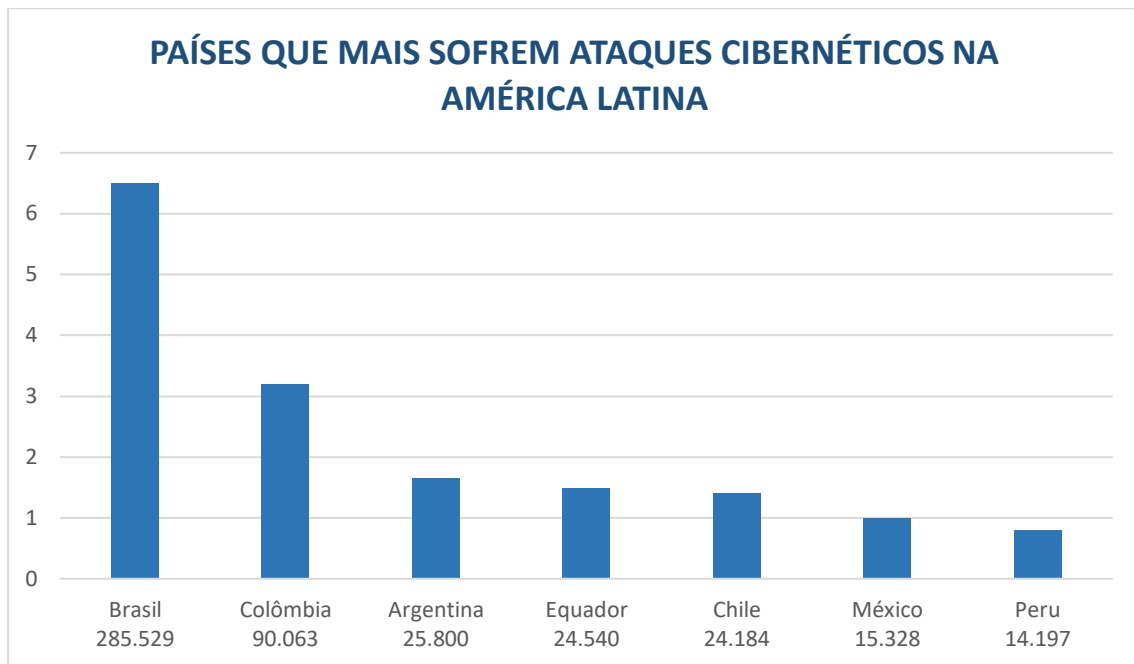
O Brasil, apesar de ser um país com avanços consideráveis no que diz respeito aos crimes virtuais, vem sendo impactado negativamente por essas práticas, distanciando-se de ser um país que progride no combate a esse tipo de crime. A empresa russa de tecnologia Kaspersky recentemente emitiu um relatório informando que o Brasil é o principal país mais afetado por golpes financeiros, além de ser destaque como o que mais é afligido com ataques de malware, totalizando em 2022, 1.554 tentativas por minuto ou 65% de todos os bloqueios na região.

Marconi (2017) afirma:

Não satisfeitos, os golpistas cibernéticos continuaram a evoluir as estratégias. Em 2022, foi observado um aumento significativo na utilização da engenharia social e do phishing para enganar as vítimas. Os ataques de phishing são uma das formas mais comuns de golpe digital bancário, com criminosos usando mensagens fraudulentas para enganar os usuários e obter informações confidenciais. Esses ataques são realizados por meio de mensagens enviadas por e-mail, SMS, redes sociais e aplicativos de mensagens, como o WhatsApp (MARCONI, 2017).

A necessidade alarmante de medidas severas é percebida ao analisar os números, destacando que nem mesmo os mais vulneráveis, como as crianças, estão imunes a essas situações. Dados da SaferNet Brasil 2023 mostram que as denúncias de conteúdos de natureza sexual envolvendo imagens de abuso de crianças e exploração sexual aumentaram 84% nos meses de janeiro a fevereiro de 2023 em comparação ao mesmo período do ano de 2022. Foram recebidas um total de 54.840 denúncias no período de 1 de janeiro a 30 de setembro do ano de 2023. Nesse sentido, o gráfico abaixo apresenta uma breve realidade dos países na América Latina:

Gráfico 1 – Realidade dos Países que na América Latina que mais sofrem ataques Cibernéticos



Fonte: Geraldo Guazzelli (2022)

Diante disso, é perceptível que o Brasil, de forma discrepante e assustadora, lidera o recorde de país com mais ataques digitais no ano de 2022 entre os países da América Latina. Um ponto importante a destacar é que Guazzelli sugere que uma das justificativas para o Brasil ocupar essa posição se deve ao fato de ser um grande produtor na área da agropecuária, abastecendo aproximadamente 15% da população mundial, o que atrai a atenção dos hackers.

Outra justificativa é o enorme crescimento em infraestrutura e atividades desde a privatização no âmbito da telecomunicação, elevando assim a posição do país no aumento desses ataques. Posto isto, conclui-se que os crimes cibernéticos impactam diversos setores da sociedade por várias razões, afetando uma ampla gama de alvos, incluindo indivíduos, empresas, instituições governamentais e organizações sem fins lucrativos.

Ninguém está imune aos riscos associados à cibercriminalidade, tornando-se cada vez mais uma preocupação persistente e crescente em nível global. Nesse tocante, observou-se também que o poder judiciário brasileiro enfrenta notável dificuldade em acompanhar as evoluções digitais. Com essa objeção, os crimes digitais que são cometidos diariamente acabam não recebendo as devidas punições, facilitando ainda mais o caminho para os cibercriminosos.

5 CONSIDERAÇÕES FINAIS

Durante toda essa pesquisa, buscou explorar as nuances do cenário digital que está em evolução constante. Ao decorrer do estudo, foram analisados aspectos cruciais que delineiam as

complexidades do crime no ciberespaço levando em consideração o seu impacto em uma sociedade cada vez mais interconectada.

Ao adentrar as intrínsecas teias da cibercriminalidade, tornou-se evidente que a ausência de fronteiras virtuais cria um ambiente propício para o caos, desafiando não apenas as estruturas tradicionais de aplicação da lei, mas também as noções convencionais de segurança e privacidade. A cada avanço tecnológico, novas brechas são abertas para explorar, resultando em uma constante dança entre agentes maliciosos e os esforços para proteger os indivíduos e instituições.

As conclusões obtidas ao longo deste estudo proporcionam uma visão aprofundada das dinâmicas da cibercriminalidade, destacando a urgência de estratégias abrangentes e colaborativas para enfrentar os desafios emergentes. As contribuições específicas deste estudo incluem: a importância de os próprios usuários da internet estarem atentos a qualquer atividade suspeita dentro desse espaço, além de realizarem precauções em suas contas e aparelhos, como: Ativar a autenticação de dois fatores para adicionar uma camada extra de proteção, manter em dia a atualizar o software, configurar senhas fortes para a rede Wi-Fi, não clicar em links suspeitos ou compartilhar informações pessoais com fontes não confiáveis.

Contudo, é imperativo reconhecer que a jornada para compreender e enfrentar a cibercriminalidade está longe de ser concluída. Visto que as fronteiras virtuais continuam a se expandir, desafiando as capacidades de proteção, integridade digital e a ordem social. Neste contexto, algumas questões emergem como postos-chave para investigações futuras, tais como: Tipos específicos de ciber Crimes, ética hacker, cibersegurança e segurança em setores específicos.

Ao mergulhar no estudo do universo digital de desafios e possibilidades, foram encontrados alguns desafios relacionados a rapidez das mudanças, a necessidade de adaptação e aprendizado constante e a importância de uma abordagem multidisciplinar. A cibercriminalidade não conhece fronteiras, e, portanto, a busca por soluções deve transcender as barreiras nacionais, envolvendo colaborações internacionais e ações coordenadas.

Em última análise, esta pesquisa pretendeu lançar compreensão a luz da natureza da cibercriminalidade, seu impacto na sociedade e as implicações para o futuro. Que as reflexões aqui apresentadas sirvam como um ponto de partida para diálogos mais amplos, inspirando ações concretas na construção de um mundo digital seguro e resiliente.

REFERÊNCIAS

BABBIE, E. **Métodos de pesquisa de survey**. Belo Horizonte: UFMG, 2016.

Brasil é o segundo país que sofre mais ataques cibernéticos na América Latina. Disponível em: <<https://br.cointelegraph.com/news/brazil-is-the-second-country-that-suffers-the-most-cyber-attacks-in-latin-america>>. Acesso em 20 set. 2023.

Brasil é o maior alvo de ataques cibernéticos na América Latina. Disponível em: <<https://oglobo.globo.com/economia/tecnologia/noticia/2023/06/brasil-e-o-maior-alvo-de-ataques-ciberneticos-na-america-latina-veja-ranking.ghml>>. Acesso em 20 set. 2023.

BRITO, AURINEY UCHOA DE. **Direito penal informático.** Editora Saraiva, São Paulo-SP, 2013.

CALDERON, B. Deep & Dark web. **A internet que você conhece é apenas a ponta do Iceberg.** Rio de Janeiro: Alta Book, 2017.

CARNEIRO, C. A. F. **Crimes Digitais:** Comentários à Lei nº 12.737/2012 (Lei Carolina Dieckmann) e Aspectos Correlatos. Juspodivm, 2018.

CASTRO, C. A. R. **Crimes digitais: Aspectos jurídicos e investigação policial.** Salvador: Juspodivm, 2015.

CRESPO, M. X. F. **Crimes digitais.** São Paulo: Saraiva, 2011. Disponível em: Minha Biblioteca.

CRESPO, X. F. **Diretivas Internacionais e Direito Estrangeiro.** Crimes Digitais. São Paulo: Saraiva, 2011.

D'URSO, L. A. F. **Cibercrime: perigo na Internet.** 2019.

Denúncias de imagens de abuso e exploração sexual infantil reportadas pela SaferNet. Disponível em: <<https://new.safernet.org.br/content/denuncias-de-imagens-de-abuso-e-exploracao-sexual-infantil-reportadas-pela-safernet>>. Acesso em 20 set. 2023.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 7ª ed. São Paulo: Atlas, 2019.

<https://www25.senado.leg.br/web/atividade/materias/-/materia/150544>, Acesso em 25 de novembro de 2023.

Influenciadora do 'Jogo do Tigre' tem bens apreendidos em operação contra jogos ilegais no Maranhão. Disponível em: <https://g1.globo.com/ma/maranhao/noticia/2023/09/26/influenciadora-do-jogo-do-tigre-tem-bens-apreendidos-em-operacao-contr-jogos-ilegais-no-maranhao.ghml>, Acesso em 17 de outubro de 2023.

INELLAS, G. C. Z. **Crimes na internet.** São Paulo: Juarez de Oliveira, 2004.

LEITE, G. S.; LEMOS, R. **Marco Civil da Internet.** Grupo GEN, 2014. Disponível em: Minha Biblioteca.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica.** São Paulo: Atlas, 2017.

NUCCI, G. S. **Manual do Direito Penal.** 10. ed.rev. atual. e ampl. Rio de Janeiro: Forense, 2014.

PECK, Patrícia. **Direito Digital**. 7ª. Ed. São Paulo: Saraiva, 2021.

RIBEIRO, L. S.; GUIMARÃES, T. A. **Cibercriminalidade: aspectos criminológicos e normativos**. Revista Brasileira de Ciências Criminais, v. 26, n. 128, p. 129-154, 2018.

ROSSINI, A. E. S. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

TEIXEIRA, Tarcisio. **Direito Digital e Processo Eletrônico**. 7ª. Ed. São Paulo: Saraiva, 2022.

TOMASEVICIUS FILHO, E. **Marco Civil da Internet: Uma lei sem conteúdo normativo**. Faculdade de Direito, Universidade de São Paulo. São Paulo/São Paulo, Brasil. 2016.

PARECER DE REVISÃO ORTOGRÁFICA E GRAMATICAL

Eu, **ALINE RODRIGUES FERREIRA**, graduada em Biblioteconomia pela Universidade Federal do Cariri, atesto que realizei a revisão ortográfica e gramatical do trabalho intitulado **“CIBERCRIMINALIDADE: O DILEMA DA SOCIEDADE ATUAL NA UTILIZAÇÃO DOS ESPAÇOS VIRTUAIS”**, de autoria de **GLENDA SLAYANE FELIX SANTOS**, sob orientação do (a) **PROF.(A) FRANCISCO GLEDSON LIMA ARAÚJO / UNILEÃO**. Declaro que este TCC está em conformidade com as normas da ABNT e apto para ser submetido à avaliação da banca examinadora de Trabalho de Conclusão de Curso do Centro Universitário Doutor Leão Sampaio/Unileão.

Juazeiro do Norte, 06/12/2023



Documento assinado digitalmente

ALINE RODRIGUES FERREIRA

Data: 08/12/2023 03:02:38-0300

Verifique em <https://validar.iti.gov.br>

ALINE RODRIGUES FERREIRA

PARECER DE TRADUÇÃO DO RESUMO PARA LINGUA INGLESA

Eu, NATHANAEL BARBOSA DA PENHA, professor(a) com formação Pedagógica em Letras: Língua Inglesa-Licenciatura, pela Instituição de Ensino Superior UNIVERSIDADE REGIONAL DO CARIRI - URCA, realizei a tradução do resumo do trabalho intitulado CIBERCRIMINALIDADE: O DILEMA DA SOCIEDADE ATUAL NA UTILIZAÇÃO DOS ESPAÇOS VIRTUAIS, do (a) aluno (a) Glenda Slayane Felix Santos e orientador (a) Francisco Gleidson Lima Araújo. Declaro que o ABSTRACT inserido neste TCC está apto à entrega e análise da banca avaliadora de Trabalho de Conclusão de Curso do Centro Universitário Doutor Leão Sampaio/Unileão.

Juazeiro do Norte, 07/12/2023



Documento assinado digitalmente

NATHANAEL BARBOSA DA PENHA

Data: 07/12/2023 12:27:18-0300

Verifique em <https://validar.iti.gov.br>

Assinatura do professor

