PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

CRIMES VIRTUAIS

A EVOLUÇÃO E A ANÁLISE DA APLICAÇÃO DO DIREITO

ORIENTANDA : NATHÁLIA VENÂNCIO DE ABREU
ORIENTADORA: Prof.ª Ms. Silvia Maria Gonçalves Santos de Lacerda Santana Curvo

GOIÂNIA-GO
2024

NATHÁLIA VENÂNCIO DE ABREU

CRIMES VIRTUAIS

A EVOLUÇÃO E A ANÁLISE DA APLICAÇÃO DO DIREITO

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC-GOIÁS).

Orientadora: ***Prof.ª. Ms. Silvia Maria Gonçalves Santos de Lacerda Santana Curvo***

GOIÂNIA-GO

2024

NATHÁLIA VENÂNCIO DE ABREU

CRIMES VIRTUAIS

A EVOLUÇÃO E A ANÁLISE DA APLICAÇÃO DO DIREITO

Data da defesa: 22 de maio de 2024 às 10:30h

BANCA EXAMINADORA

Orientadora: Prof.ª. Ms. Silvia Maria Gonçalves Santos de Lacerda Santana Curvo

Nota:

Examinadora Convidada: Eufrosina Saraiva Silva

Nota:

SUMÁRIO

CRIMES VIRTUAIS

A EVOLUÇÃO E A ANÁLISE DA APLICAÇÃO DO DIREITO

Nathália Venâncio de Abreu[1]

Prof.ª: Ms. Silvia Maria Gonçalves Santos de Lacerda Santana Curvo [2]

Resumo: O presente trabalho visa explorar os crimes virtuais, a sua evolução e a análise da aplicação do direito nessa temática. Este objeto aborda a crescente complexidade dos delitos virtuais em um cenário tecnológico em constante evolução, bem como a forma como o sistema jurídico tem respondido a esses desafios. Ao longo deste trabalho, serão examinados a história e o desenvolvimento dos crimes virtuais, suas implicações sociais, econômicas e éticas, assim como as estratégias legais e de aplicação da lei empregadas para combatê-los. O escopo deste estudo se concentra na análise dos crimes virtuais em um contexto nacional específico e nas estratégias legais e de aplicação da lei adotadas para enfrentá-los. Pretende-se, por meio dessa pesquisa, realizar uma análise aprofundada dessas questões, contribuindo para um entendimento mais amplo e abrangente do tema em questão.

Palavras-chaves: Crimes Virtuais. Evolução da Legislação. Crimes Cibernéticos.

Abstract: This work aims to explore virtual crimes, their evolution and the analysis of the application of law on this topic. This object addresses the growing complexity of virtual crimes in a constantly evolving technological scenario, as well as the way in which the legal system has responded to these challenges. Throughout this work, the history and development of virtual crimes, their social, economic and ethical implications, as well as the legal and law enforcement strategies employed to combat them, will be examined. The scope of this study focuses on the analysis of cybercrimes in a specific national context and the legal and law enforcement strategies adopted to address them. The aim of this research is to carry out an in-

[1] Graduanda no curso de Direito pela Pontifícia Universidade Católica do Estado de Goiás.

[2] Doutoranda pela Universidade de Salamanca- ES, mestre em Direito Agrário pela UFG- Universidade Federal de Goiás (2002), bacharel em Direito pela Pontifícia Universidade Católica de Goiás (1993), graduação em Pedagogia pela Pontifícia Universidade Católica de Goiás (1983). Especializações em: Direito Penal, Direito Civil, Direito Processual Civil, Direito Constitucional. Atualmente é professora assistente da Pontifícia Universidade Católica de Goiás PUC/GO.

depth analysis of these issues, contributing to a broader and more comprehensive understanding of the topic in question.
Keywords: Virtual Crimes. Evolution of Legislation. Cyber Crimes.

INTRODUÇÃO

No contexto contemporâneo, a ubiquidade da tecnologia e a crescente interconexão digital proporcionaram uma revolução nas formas de interação social, comunicação e transações. Paralelamente a essa era de inovação, emergem desafios intrínsecos à sociedade da informação, dando origem a uma categoria de delitos que transcende as fronteiras físicas: os crimes virtuais.

O presente trabalho propõe-se a uma análise minuciosa e crítica dessa evolução, explorando a interação dinâmica entre o avanço tecnológico e a eficácia das estratégias jurídicas na contenção dessas transgressões.

Os crimes virtuais, também conhecidos como cibercrimes, englobam uma ampla gama de atividades ilícitas praticadas através de meios eletrônicos, tais como fraudes online, ataques de hackers, disseminação de vírus e invasão de privacidade. Esses delitos apresentam desafios únicos devido à sua natureza global, dinâmica e muitas vezes sofisticada, exigindo respostas ágeis e adaptáveis por parte das autoridades e do sistema jurídico.

Ao longo deste trabalho, serão explorados diversos aspectos relacionados aos crimes virtuais. Inicialmente, será realizada uma análise da evolução histórica desses delitos, desde suas origens até as formas mais contemporâneas de ataques cibernéticos. Em seguida, serão examinadas as implicações sociais, econômicas e éticas associadas aos crimes virtuais, destacando seus impactos sobre a sociedade e as organizações.

Posteriormente, serão abordadas as estratégias legais e de aplicação da lei utilizadas para enfrentar os crimes virtuais, incluindo a legislação específica, os desafios enfrentados pelas autoridades na investigação e punição dos infratores, e as iniciativas de cooperação internacional para combater a criminalidade online.

Por fim, este trabalho pretende contribuir para um debate mais amplo e informado sobre os crimes virtuais, fornecendo insights relevantes para a compreensão de sua dinâmica e para o aprimoramento das políticas públicas e práticas jurídicas voltadas para sua prevenção e repressão.

1 CRIMES VIRTUAIS E O SEU SURGIMENTO

A globalização e a evolução das tecnologias desempenham papéis cruciais no cenário atual, especialmente no contexto dos crimes virtuais. A interconexão global proporcionada pela internet e pelas tecnologias de comunicação permitiu uma integração sem precedentes entre países, organizações e indivíduos. No entanto, essa mesma interconexão também trouxe consigo novos desafios e vulnerabilidades, que são explorados por criminosos virtuais em todo o mundo.

Um exemplo marcante da interação entre globalização e tecnologia é o surgimento das redes sociais. Plataformas como Facebook, Twitter e Instagram conectam bilhões de pessoas em todo o mundo, facilitando a comunicação e o compartilhamento de informações. No entanto, essas mesmas plataformas também se tornaram alvos para atividades criminosas, como a disseminação de spam, phishing e fraudes online.

Além disso, a globalização e a evolução das tecnologias deram origem a novas formas de crime, como o ransomware. Essa modalidade de crime virtual envolve o sequestro de dados por meio de software malicioso, com os criminosos exigindo resgate para liberar o acesso aos arquivos. O ransomware é um exemplo claro de como a tecnologia pode ser utilizada de maneira maliciosa para extorquir indivíduos e organizações em escala global.

Outro exemplo importante é o uso de tecnologias de criptografia para ocultar atividades criminosas online. A criptografia é uma ferramenta essencial para proteger a privacidade e a segurança das comunicações na internet, mas também pode ser utilizada por criminosos para ocultar suas identidades e atividades ilícitas. Isso cria desafios significativos para as autoridades na investigação e combate aos crimes virtuais, especialmente em um contexto internacional. Oportunamente, o direito à privacidade é garantido no artigo 5º, X da Constituição Federal do Brasil:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> …
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Em suma, o artigo 5º, inciso X, da Constituição Federal do Brasil, desempenha um papel fundamental na proteção dos direitos individuais, garantindo a

preservação da intimidade, da vida privada, da honra e da imagem das pessoas, e reafirmando o compromisso do Estado brasileiro com a dignidade humana e com os princípios democráticos.

Em suma, a globalização e a evolução das tecnologias têm influenciado profundamente o cenário dos crimes virtuais, proporcionando novas oportunidades para os criminosos e desafios adicionais para as autoridades e o sistema jurídico. É essencial entender essas dinâmicas em constante evolução para desenvolver estratégias eficazes de prevenção e repressão dos crimes virtuais em um contexto globalizado e altamente tecnológico. Portanto, o Brasil, demorou de maneira significante a tratar sobre esse assunto, nesse sentido, Carneiro (2012) esclarece que:

> "O Brasil começou a se preocupar com esse assunto especialmente a partir das últimas décadas, com o aumento da popularização dessa inovação tecnológica, promulgando, na Constituição Federal de 1988, leis relativas à competência do Estado sobre questões de informática".

Essa atenção crescente do Brasil para com a informática na esfera constitucional reflete não apenas uma resposta às mudanças tecnológicas, mas também uma preocupação com a proteção dos direitos individuais, a promoção da inovação e o desenvolvimento econômico sustentável. Portanto, a inclusão de leis sobre informática na Constituição Federal de 1988 marca um marco importante na evolução do ordenamento jurídico brasileiro, alinhando-o com as demandas e desafios da sociedade digital.

1.1 CLASSIFICAÇÃO DOS CRIMES VIRTUAIS

Na esfera jurídica, a classificação dos crimes virtuais pode ser abordada sob a ótica da sua natureza e características, sendo comumente categorizados em três grupos distintos: crimes virtuais puros, impuros e mistos. Portanto, os pensamentos estendem a vários doutrinadores, nesse sentido Pinheiro (FERREIRA, 2001), esclarece que deve levar em consideração o papel desempenhado pelo meio utilizado para praticar o crime:

> "(...) 1) quando o computador é o alvo – p. Ex.: crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação de conteúdo do banco de dados, furto de informação, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo por fora da empresa; 2) quando computador é o instrumento para o crime – ex.: crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraude de telecomunicações, divulgação ou exploração de pornografia; 3) quando o computador é incidental para outro crime – ex.: crimes contra honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, registro de atividades do crime organizado; 4) quando o crime está associado

> com computador – p. Ex.: pirataria de software, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas de comércio ilegal de equipamentos e programas”

Em suma, o trecho apresenta uma visão abrangente dos diferentes papéis que os computadores desempenham na perpetração de crimes, sublinhando a complexidade e a evolução das ameaças cibernéticas e a necessidade contínua de adaptação e aprimoramento das leis e práticas de segurança cibernética.

Os crimes virtuais puros referem-se àqueles que são exclusivamente perpetrados no ambiente digital, sem a necessidade de uma interação física direta entre o criminoso e a vítima. São exemplos claros de crimes virtuais puros aqueles em que a conduta criminosa ocorre integralmente em meio eletrônico, sem qualquer envolvimento presencial.

Já os crimes virtuais impuros são caracterizados pela utilização do meio digital como parte do processo delitivo, mas com uma conexão direta com ações ou consequências no mundo físico. Um exemplo clássico é o crime de estelionato praticado por meio de transações fraudulentas realizadas online, que têm impacto direto sobre o patrimônio da vítima no mundo real. Nesse caso, o elemento virtual é um instrumento utilizado pelo criminoso para facilitar a prática do delito, mas a lesão efetiva ocorre no ambiente físico.

Por fim, os crimes virtuais mistos envolvem uma combinação de elementos virtuais e físicos, em que tanto a conduta criminosa quanto as suas consequências se manifestam em ambos os domínios. Um exemplo típico são os casos de cyberbullying, em que agressões verbais ou difamações são perpetradas por meio de redes sociais ou mensagens eletrônicas, mas causam danos emocionais e psicológicos reais para a vítima no mundo físico, causando traumas imensuráveis.

Essa classificação dos crimes virtuais permite uma compreensão mais detalhada e precisa das diferentes formas de condutas ilícitas que ocorrem no ambiente digital, possibilitando a adoção de estratégias e medidas legais adequadas para sua prevenção e repressão.

2 LEGISLAÇÃO E JURISPRUDÊNCIA

A sociedade passa a maior parte do tempo conectada nos ambientes virtuais, para isso é necessário a existência de leis que garantam a ordem social, de

maneira que os princípios e garantias sejam obedecidos. A conjuntura dos crimes virtuais no panorama jurídico brasileiro evoluiu de maneira notável nas últimas décadas, demandando uma análise criteriosa tanto da legislação pertinente quanto das decisões judiciais que moldam a aplicação do direito nesse domínio. Ao explorarmos essa complexa relação entre a legislação e a jurisprudência, este estudo visa lançar luz sobre os desafios e avanços na contenção dos crimes virtuais.

As leis e regulamentos relacionados à cibersegurança e crimes virtuais têm evoluído para acompanhar as novas ameaças. No entanto, os criminosos virtuais também se adaptam às mudanças na legislação, encontrando maneiras de contornar as restrições legais.

2.1 LEGISLAÇÃO RELACIONADA A CRIMES VIRTUAIS EM SUA JURISDIÇÃO.

A legislação brasileira sobre crimes virtuais tem sua base primordial na Lei nº 12.737/2012, comumente conhecida como a "Lei Carolina Dieckmann", um caso de grande repercussão midiática, lei que foi publicada no dia 30 de novembro de 2012, e o início de sua vigência foi 120 dias depois, que dispõe sobre a tipificação dos delitos informáticos e a invasão de dispositivo:

> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B

Esta legislação representa um marco crucial ao tipificar crimes cibernéticos, abrangendo desde invasões de dispositivos informáticos até a obtenção não autorizada de dados digitais. Adicionalmente, o Código Penal Brasileiro foi modificado para incluir disposições específicas relacionadas a delitos cometidos no ambiente virtual.

Ainda nesse contexto, o Código Penal traz na parte mais significativa dos crimes virtuais os artigos citados na Lei Carolina Dieckmann:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública

> direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Esses referidos artigos tratam das penalidades impostas aos crimes de invasão de dispositivo, que são boa parte dos crimes cibernéticos atuais e são uma base para enfrentar desafios ao longo da globalização.

É imperioso citar a Lei 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no nosso país, lei publicada em 23 de abril de 2014 que entrou em vigor 60 dias após a sua publicação oficial.

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - Inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

Lei que se refere principalmente a liberdade de expressão e os princípios conservadores, esta legislação deveria em tese ser mais conhecida e mais comentada, tendo em vista que toda a sociedade utiliza a internet diariamente e na maioria do tempo.

Ademais, é de extrema importância a criação de legislações mais severas em relação esse tipo de crime, tendo em vista que a cada ano o número de pornografia infantil, conteúdos de apologia à violência e ao crime e a honra, e a violência contra a mulher cresce exorbitantemente. É plausível falarmos também do crime de estelionato que é um dos crimes mais cometidos na sociedade brasileira e que cresce de maneira exorbitante e acontece principalmente no ambiente virtual:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. (Vide Lei nº 7.209, de 1984)
> § 1º ...
> § 2º - Nas mesmas penas incorre quem:
> I - ...
> II - ...
> III - ...
> IV - ...
> V - ...
> VI - ...
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

Em suma, o Artigo 171 do Código Penal desempenha um papel fundamental na proteção do patrimônio e na preservação da confiança nas relações comerciais e sociais. Sua aplicação efetiva contribui para a promoção da justiça e para a segurança jurídica, garantindo que os responsáveis por atos fraudulentos sejam responsabilizados de acordo com a lei.

Contudo, a evolução rápida da tecnologia frequentemente supera a capacidade da legislação em manter-se atualizada. A constante inovação no campo digital desafia a rigidez da linguagem legal, destacando a necessidade de revisões e adaptações constantes para cobrir lacunas emergentes.

2.2 ANÁLISE CRÍTICA DAS LEIS

A análise crítica das leis relacionadas a crimes virtuais é crucial para uma compreensão aprofundada de sua eficácia e adequação. A interpretação e aplicação dessas leis pelos tribunais moldam a jurisprudência, desempenhando um papel fundamental na orientação do sistema jurídico em resposta às dinâmicas complexas do ciberespaço.

As decisões judiciais refletem não apenas a aplicação das leis existentes, mas também a interpretação dos magistrados sobre questões como privacidade, responsabilidade e proporcionalidade das sanções. Contudo, surgem desafios interpretativos, especialmente quando confrontados com as rápidas mudanças tecnológicas e a multiplicidade de situações únicas que os crimes virtuais podem apresentar. Abaixo, destaco alguns casos notórios e apresento breves análises jurídicas associadas a cada um:

Em 2016, houve o caso da Carolina Dieckmann, a atriz teve seu computador invadido, resultando no roubo de fotos íntimas. Os criminosos exigiram dinheiro para não divulgar as imagens. Então, a atriz teve suas fotos íntimas pessoais divulgados na internet sem sua autorização. O caso levantou debates sobre a adequação da legislação existente para tratar desse tipo de crime.

À época, a Lei Carolina Dieckmann (Lei nº 12.737/2012) foi promulgada para tipificar delitos informáticos, incluindo invasão de dispositivo e divulgação não autorizada de imagens. A extorsão envolvendo a demanda por dinheiro para não divulgar as imagens levou a questões relacionadas à extorsão virtual e a interpretação

desses atos sob a legislação vigente. A investigação focou na identificação dos responsáveis, destacando os desafios da jurisdição e cooperação internacional em casos de crimes virtuais.

O caso Carolina Dieckmann desempenhou um papel fundamental na conscientização sobre crimes virtuais e na criação de instrumentos legais mais eficazes para lidar com essas situações. Além da lei que leva seu nome, o episódio contribuiu para fortalecer o entendimento sobre a seriedade desses delitos e a necessidade de proteger a privacidade digital. A análise jurídica desse caso destaca como a legislação precisa evoluir em resposta aos desafios emergentes no mundo digital, garantindo que haja instrumentos eficazes para responsabilizar os perpetradores e proteger os direitos das vítimas de crimes virtuais.

Em 2017, ocorreu o caso WannaCry, um ataque de ransomware afetou sistemas globais, incluindo serviços de saúde e infraestrutura crítica. As análises jurídicas abordaram a criminalização do uso de ransomware, a cooperação internacional na identificação dos perpetradores e as implicações legais para organizações negligentes na proteção contra os ataques.

Em 2019, teve o caso de hacker que invadiu celulares de autoridades, incluindo o então Ministro da Justiça, Sergio Moro. Este caso levantou questões sobre a segurança cibernética de autoridades e a necessidade de aprimorar a legislação para enfrentar ataques direcionados. A análise jurídica incluiu discussões sobre a tipificação de crimes cibernéticos e os limites da privacidade em casos de interesse público.

Em 2021, teve o caso do vazamento de dados de mais de 220 milhões de brasileiros foram vazados após um ataque à Serasa Experian. Este caso suscitou debates sobre a segurança dos dados pessoais e a responsabilidade das empresas na proteção dessas informações. A análise jurídica incluiu discussões sobre a Lei Geral de Proteção de Dados (LGPD) e as consequências legais para violações de dados em massa.

Esses casos refletem a diversidade de desafios enfrentados pela legislação brasileira no âmbito dos crimes virtuais, destacando a necessidade contínua de adaptação da legislação e jurisprudência para lidar com as complexidades do ambiente digital. A análise jurídica desses casos contribui para o aprimoramento das estratégias legais e da proteção aos cidadãos no contexto digital.

3 COOPERAÇÃO INTERNACIONAL

A crescente interconexão global trouxe consigo não apenas benefícios, mas também desafios, especialmente no que diz respeito aos crimes virtuais. Uma das principais dificuldades enfrentadas pelas autoridades é a natureza transnacional dos crimes virtuais.

Os criminosos podem operar em um país enquanto visam alvos em outro, utilizando servidores e infraestrutura localizada em jurisdições diferentes. Isso levanta questões sobre qual jurisdição tem autoridade para investigar e processar esses crimes.

A cooperação internacional é um elemento fundamental no enfrentamento desses delitos, visto que muitas vezes transcendem fronteiras nacionais. Neste contexto, a legislação e jurisprudência brasileiras desempenham um papel crucial, sendo influenciadas por tratados, acordos e desafios inerentes à colaboração internacional. Enquanto lutam contra o crime cibernético, as autoridades devem garantir o respeito aos direitos humanos, incluindo a privacidade, a liberdade de expressão e o devido processo legal. O equilíbrio entre a segurança cibernética e os direitos individuais é uma consideração crucial em todas as etapas da aplicação da lei.

3.1 ACORDOS, CONVENÇÕES E TRATADOS INTERNACIONAIS RELACIONADOS AO CRIME CIBERNÉTICO

As leis e regulamentos variam significativamente entre os países, o que pode criar barreiras jurisdicionais para a aplicação da lei em casos de crimes virtuais. Além disso, alguns países podem ter leis mais permissivas ou lacunas legais que os criminosos exploram para evitar a responsabilidade legal.

A cooperação internacional no combate a crimes virtuais é fundamentada em uma rede de tratados e acordos que buscam facilitar a troca de informações, provas e ações conjuntas entre países. Exemplos incluem a Convenção de Budapeste sobre Crime Cibernético e a Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo), ambos ratificados pelo Brasil. Esses instrumentos estabelecem diretrizes para a cooperação no âmbito cibernético, proporcionando uma base legal para a atuação conjunta contra crimes virtuais.

Desta forma, é imprescindível a análise da Convenção da Budapeste que foi promulgada em abril de 2023, pelo Vice-Presidente da época, Geraldo José Rodrigues Alckmin Filho e principalmente os artigos 23 e 29 que se referem a cooperação internacional e a assistência mútua nesta convenção:

> Art. 23º As Partes cooperarão entre si, de acordo com as disposições deste capítulo, e por meio da aplicação de instrumentos internacionais pertinentes de cooperação internacional em assuntos penais, de ajustes firmados com base em legislação uniforme ou de reciprocidade, e da legislação doméstica, o mais possível, para a realização das investigações ou procedimentos acerca de crimes de computador, ou para a coleta de provas eletrônicas desses crimes.
> …
> Art. 29º 1. Qualquer Parte pode pedir a outra Parte que determine a obtenção ou de qualquer modo obtenha a expedita conservação de dados armazenados por meio de um sistema de computador, localizado no território daquela outra Parte, em relação aos quais a Parte requerente pretende apresentar um pedido de assistência mútua para busca ou acesso, apreensão ou guarda, ou revelação dos dados.

A implementação desses artigos requer um equilíbrio cuidadoso entre a eficácia na aplicação da lei e a proteção dos direitos dos cidadãos, refletindo os desafios contínuos no campo da segurança cibernética e da governança da Internet.

Ainda no contexto de convenção internacional, é possível citar o artigo 18 da Convenção de Palermo, que foi promulgada em 2004 pelo Lula Inácio da Silva, presidente no referido ano, que trata da cooperação internacional e assistência juridica:

> Art. 18º 1. Os Estados Partes prestarão reciprocamente toda a assistência judiciária possível nas investigações, nos processos e em outros atos judiciais relativos às infrações previstas pela presente Convenção, nos termos do Artigo 3, e prestarão reciprocamente uma assistência similar quando o Estado Parte requerente tiver motivos razoáveis para suspeitar de que a infração a que se referem as alíneas a) ou b) do parágrafo 1 do Artigo 3 é de caráter transnacional, inclusive quando as vítimas, as testemunhas, o produto, os instrumentos ou os elementos de prova destas infrações se encontrem no Estado Parte requerido e nelas esteja implicado um grupo criminoso organizado.

A implementação efetiva deste artigo requer uma infraestrutura jurídica robusta, bem como mecanismos claros e eficientes para a comunicação e execução de solicitações de assistência. Além disso, a confiança mútua e a vontade política dos Estados Partes são essenciais para garantir que a assistência jurídica mútua seja eficaz na prática, contribuindo significativamente para a prevenção e repressão do crime organizado transnacional.

3.2 EXEMPLO DE CASO DE COOPERAÇÃO INTERNACIONAL NA INVESTIGAÇÃO E PROTEÇÃO DE CRIMES VIRTUAIS.

No âmbito brasileiro, casos como a “Operação Lava Jato", que foi uma das maiores investigações de combate a corrupção e a lavagem de dinheiro na história do Brasil, que se iniciou em 2014, visava investigar agentes públicos, empresários, e até mesmo doleiros, e essa operação revela a importância da cooperação com outros países na investigação de crimes cibernéticos associados a corrupção e lavagem de dinheiro.

3.3 DESAFIOS E BARREIRAS A COOPERAÇÃO INTERNACIONAL

Apesar dos avanços, diversos desafios persistem na cooperação internacional contra crimes virtuais. Barreiras culturais, diferenças jurídicas e procedimentais, bem como questões de soberania nacional, podem dificultar a efetividade da colaboração. Além disso, a rapidez com que ocorrem os ataques cibernéticos muitas vezes contrasta com os procedimentos burocráticos, criando um desafio adicional para a ação coordenada. Nesse sentido, Barbosa (CALIXTO, 2023) retrata que:

> Um dos principais desafios é a dificuldade de identificação dos criminosos. Os crimes virtuais podem ser realizados por meio de técnicas de anonimização, dificultando a identificação do autor do crime. Além disso, muitas vezes os criminosos utilizam técnicas de hackinge phishing, invadindo sistemas e roubando informações de usuários, o que dificulta ainda mais a identificação do criminoso. Outro desafio é a falta de harmonização das leis entre os países.

Os desafios na identificação de criminosos virtuais e a falta de harmonização das leis entre os países exigem uma abordagem multifacetada e colaborativa. A abordagem coordenada e integrada, combinando avanços tecnológicos, harmonização jurídica e cooperação internacional, é crucial para enfrentar os desafios impostos pelos crimes cibernéticos no cenário global atual.

A preservação da privacidade e proteção de dados pessoais também emerge como um ponto sensível na cooperação internacional. A diversidade de normas de privacidade entre os países muitas vezes demanda esforços significativos para harmonizar abordagens e garantir o respeito aos direitos individuais durante investigações transnacionais.

No contexto em constante evolução dos crimes virtuais, a cooperação internacional continuará desempenhando um papel crucial. A superação dos desafios exige uma abordagem multissetorial, envolvendo governos, setor privado e organizações internacionais.

4 AVANÇO TECNOLÓGICO E INVESTIGAÇÃO

A partir da década de 1990, a internet experimentou um crescimento explosivo com o surgimento de serviços populares como e-mail, navegadores web, motores de busca e redes sociais. Desde então, a internet tem se tornado cada vez mais integrada à vida cotidiana das pessoas em todo o mundo, conforme dados da Valor Econômico Globo (DINO, 2023):

> Atualmente, o país enfrenta uma verdadeira epidemia de crimes cibernéticos, afetando cidadãos, empresas e até mesmo instituições governamentais. De acordo com um estudo realizado pelo laboratório de inteligência e ameaças, FortiGuard Labs, e publicado pela CNN, somente no primeiro semestre de 2022, o país sofreu cerca de 31,5 bilhões de tentativas de ataques cibernéticos, representando um aumento de 94% em relação aos 16,2 bilhões do ano anterior.

Atualmente, o país está enfrentando uma verdadeira epidemia de crimes cibernéticos, que tem afetado significativamente cidadãos, empresas e instituições governamentais. Esta situação alarmante é corroborada por um estudo realizado pelo FortiGuard Labs, um laboratório de inteligência e ameaças, e publicado pela CNN, revelando dados preocupantes sobre o aumento das tentativas de ataques cibernéticos.

O avanço tecnológico, embora traga inúmeras vantagens para a sociedade, também representa um terreno fértil para o desenvolvimento de crimes virtuais cada vez mais sofisticados. No contexto brasileiro, o impacto do avanço tecnológico na evolução dos crimes virtuais é evidente, demandando métodos e técnicas de investigação igualmente avançados para enfrentar esses desafios. Ainda, nesse quesito declara BRITZ (2009 apud Barreto, Silva e Kufa, 2020, p.49):

> “No entanto, o advento da tecnologia reduziu as barreiras tradicionais e, em verdade, serviu como um convite informal a visitantes desconhecidos. Muitos perceberam tarde demais os perigos de sua desatenção e se tornaram vítimas de furto, da perda de dados privados e similares. Outros permanecem ignorantes de sua vulnerabilidade, prestes a sofrerem as consequências de sua postura.”

A citação de Britz destaca de maneira eloquente a transformação e os desafios introduzidos pela tecnologia na esfera da segurança pessoal e corporativa. O advento da tecnologia, enquanto facilitador de inúmeras atividades e inovações, também reduziu as barreiras tradicionais, expondo usuários a novos tipos de ameaças. A reflexão de Britz aponta para um paradoxo inerente: a tecnologia, que visa simplificar e melhorar a vida das pessoas, também pode servir como uma porta aberta para criminosos cibernéticos.

4.1 IMPACTO DO AVANÇO TECNOLÓGICO NA EVOLUÇÃO DOS CRIMES VIRTUAIS

O Brasil, como uma das nações em desenvolvimento tecnológico acelerado, testemunhou uma transformação significativa na paisagem dos crimes virtuais. O aumento da conectividade, o crescimento das transações online e a proliferação de dispositivos conectados ampliaram o espectro de oportunidades para criminosos digitais. Desde ataques de ransomware a esquemas de phishing mais elaborados, o avanço tecnológico tem sido um catalisador para a sofisticação dos métodos empregados pelos criminosos. Outrossim, para Torres (Claudio, 2009, p.24):

> Novas tecnologias e aplicações, como os blogs, as ferramentas de buscas, os fóruns, as redes sociais e tantas outras aplicações on-line foram utilizadas pelos internautas para, literalmente, assumir o controle, a produção e o consumo da informação, atividades antes restritas aos grandes portais.

A citação de Claudio Torres captura a essência de uma revolução na produção e consumo de informação impulsionada pela tecnologia. A capacidade dos internautas de assumir o controle destas atividades anteriormente dominadas por grandes portais representa tanto oportunidades quanto desafios. O empoderamento individual e a democratização da informação têm o potencial de enriquecer o discurso público e promover a diversidade, mas também exigem uma abordagem consciente e responsável por parte dos usuários e das plataformas. Adaptar-se a este novo panorama é essencial para maximizar os benefícios enquanto se minimizam os riscos associados à desinformação.

Com o aumento tecnológico, consequentemente, os crimes virtuais foram se incidindo, começando-os com fraude por meio de e-mails, sites falsos que traziam vírus para os equipamentos dos usuários, pornografias, piratarias. A disseminação de tecnologias emergentes, como inteligência artificial e blockchain, também introduz

novos desafios. O anonimato proporcionado por criptomoedas e a capacidade de automatizar ataques exigem uma resposta igualmente inovadora por parte das autoridades e profissionais da segurança. E, ainda com o aumento da conectividade e do uso da internet, os alvos dos crimes virtuais se tornaram mais diversos e abrangentes.

O avanço da tecnologia, incluindo o surgimento de deepfakes, inteligência artificial (IA) e ataques à infraestrutura crítica, tem apresentado desafios significativos para o campo jurídico. Diante dessas novas ameaças, o direito tem buscado se adaptar e desenvolver estratégias para lidar com essas questões emergentes.

Os deepfakes, que são vídeos ou imagens manipuladas digitalmente para parecerem autênticos, representam um desafio para a autenticidade e veracidade das evidências em processos judiciais. O direito tem respondido a essa ameaça através da análise cuidadosa das provas digitais, promovendo a adoção de métodos de autenticação mais robustos e investindo em tecnologias de detecção de deepfakes.

A inteligência artificial (IA) também levanta questões legais complexas, especialmente no contexto da responsabilidade por decisões automatizadas. O direito tem explorado questões relacionadas à transparência, responsabilidade e ética no uso de algoritmos e sistemas de IA em processos judiciais, visando garantir a equidade e a imparcialidade nas decisões judiciais.

Os ataques à infraestrutura crítica, como sistemas de energia, transporte e comunicações, representam uma ameaça significativa à segurança nacional e à estabilidade social. O direito tem respondido a essa ameaça através do desenvolvimento de leis e regulamentos que visam proteger e fortalecer a infraestrutura crítica contra ataques cibernéticos, além de promover a cooperação internacional para enfrentar essas ameaças transnacionais.

Em suma, o direito tem desempenhado um papel crucial na adaptação e resposta aos desafios apresentados pela evolução tecnológica, incluindo deepfakes, inteligência artificial e ataques à infraestrutura crítica. Através da análise cuidadosa das implicações legais dessas tecnologias emergentes e da implementação de medidas regulatórias apropriadas, o direito busca garantir a proteção dos direitos individuais, a segurança pública e a estabilidade social em um mundo digital em constante mudança.

4.2 MÉTODOS E TÉCNICAS DE INVESTIGAÇÃO AVANÇADAS.

A resposta efetiva aos crimes virtuais requer uma atualização constante dos métodos de investigação. A análise forense digital, por exemplo, tornou-se uma peça fundamental na identificação de evidências digitais, envolvendo a recuperação e análise de dados em dispositivos eletrônicos. Técnicas avançadas de rastreamento de transações financeiras digitais também se tornaram cruciais na investigação de crimes como lavagem de dinheiro virtual.

A colaboração com especialistas em segurança cibernética, o uso de ferramentas de inteligência artificial para análise de padrões e a implementação de tecnologias de monitoramento em tempo real são estratégias que acompanham a evolução dos métodos criminosos.

Ainda nesse contexto, é de extrema importância a infiltração virtual de agentes, que está instituída na Lei Anticrime (Lei 13.964/2019), na Lei de Drogas (Lei nº 11.343, de 23 de agosto de 2006), na Lei de Organizações Criminosas (Lei nº 12.850, de 2 de agosto de 2013), na Convenção de Palermo e ainda na mais atual alteração no Estatuto da Criança e do Adolescente (Lei nº 13.441, de 8 de maio de 2017).

Em suma, referindo os termos da Lei nº 12.850, de 2 de agosto de 2013, que discorre sobre a definição da organização criminosa e trata sobre investigação criminal e meios de obtenção de prova:

> Art. 10-A. Será admitida a ação de agentes de polícia infiltrados virtuais, obedecidos os requisitos do caput do art. 10, na internet, com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.

O Artigo 10-A da Lei nº 12.850, de 2 de agosto de 2013, representa um avanço significativo no combate às organizações criminosas, ao formalizar os acordos de não persecução penal. Este mecanismo contribui para a eficiência e eficácia das investigações criminais, promovendo a colaboração dos investigados em troca de benefícios legais. As garantias processuais e os requisitos estabelecidos no artigo asseguram a integridade e a legalidade dos acordos, protegendo os direitos dos colaboradores e fortalecendo o sistema judicial na luta contra o crime organizado.

Ademais, a grande potência mundial atual, ou seja, Estados Unidos, desenvolveu o Tor que significa “The Onion Routing”, traduzindo para o português: roteamento de cebola, por se tratar das camadas dentro do sistema operacional, para burlar a falta de segurança, sendo o maior Dark Web já desenvolvido, serve para navegar normalmente na internet, portanto de forma privada. Esse software ganhou muita popularidade, por garantir a anonimidade e segurança.

5 EVOLUÇÃO DAS PENAS E SANÇÕES

A evolução das penas e sanções no contexto dos crimes virtuais é um aspecto crucial a ser considerado na análise da aplicação do direito nessa área em constante transformação. Ao longo do tempo, a legislação tem passado por mudanças significativas para acompanhar o avanço das tecnologias e as novas formas de delitos que surgem no ciberespaço.

5.1 PENAS E SANÇÕES PREVISTAS PARA CRIMES VIRTUAIS.

As penas e sanções previstas para crimes virtuais variam de acordo com a natureza e gravidade do delito. Em muitos países, a legislação prevê penas que vão desde multas e detenção até penas de prisão, dependendo do tipo de crime e dos danos causados. Por exemplo, a invasão de dispositivos informáticos pode resultar em detenção de três meses a um ano, além de multa, de acordo com o artigo 154-A do Código Penal brasileiro.

Além disso, temos também o crime de Stalking, muito comum atualmente:

> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.
> § 1º A pena é aumentada de metade se o crime é cometido:
> I – contra criança, adolescente ou idoso;
> II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código;
> III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.
> § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência.

O Artigo 147-A do Código Penal Brasileiro representa um marco importante na proteção dos direitos individuais contra a perseguição. Ao tipificar o stalking como

crime, a legislação brasileira avança na defesa da integridade física e psicológica das pessoas, proporcionando mecanismos claros e específicos para coibir comportamentos abusivos e intrusivos. As disposições sobre as circunstâncias agravantes e a aplicabilidade das penas sem prejuízo de outras correspondentes à violência reforçam a seriedade do crime e a necessidade de uma resposta judicial efetiva. Ainda na análise de penas referentes ao tema, presentes ainda no Código Penal, temos o cyberbullyng:

> Art. 146-A. Intimidar sistematicamente, individualmente ou em grupo, mediante violência física ou psicológica, uma ou mais pessoas, de modo intencional e repetitivo, sem motivação evidente, por meio de atos de intimidação, de humilhação ou de discriminação ou de ações verbais, morais, sexuais, sociais, psicológicas, físicas, materiais ou virtuais:
> Parágrafo único. Se a conduta é realizada por meio da rede de computadores, de rede social, de aplicativos, de jogos on-line ou por qualquer outro meio ou ambiente digital, ou transmitida em tempo real:
> Pena - reclusão, de 2 (dois) anos a 4 (quatro) anos, e multa, se a conduta não constituir crime mais grave.

O Artigo 146-A do Código Penal Brasileiro representa um avanço significativo na proteção contra a intimidação sistemática, reconhecendo a diversidade de formas que o bullying e o assédio podem assumir, tanto no mundo físico quanto digital. A penalização severa reflete a gravidade com que a sociedade deve tratar esses comportamentos, oferecendo um recurso legal robusto para as vítimas e promovendo um ambiente mais seguro e respeitoso. Este artigo também destaca a necessidade de uma abordagem integrada e colaborativa para a prevenção e combate ao bullying, envolvendo tanto políticas públicas quanto iniciativas educacionais e sociais.

Em suma, a evolução das penas e sanções para crimes virtuais reflete a necessidade de uma resposta jurídica eficaz a essas ameaças em constante evolução, demonstrando a importância da análise crítica da legislação ao longo do tempo para entender melhor a aplicação do direito nesse campo específico.

5.2 MUDANÇAS NA LEGISLAÇÃO AO LONGO DO TEMPO.

A Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) foi inspirada em regulamentações internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, e reflete a crescente conscientização sobre a importância da proteção de dados no contexto atual. A referida lei discorre:

> 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.

No contexto dos crimes virtuais, a LGPD desempenha um papel crucial na proteção dos dados pessoais dos indivíduos contra ações maliciosas e violações de segurança. Ao estabelecer regras claras para o tratamento de dados pessoais por parte das organizações, a lei busca mitigar os riscos de violações de dados e proteger a privacidade dos usuários.

6 CIBERSEGURANÇA E PREVENÇÃO

Cibersegurança é um conjunto de práticas, políticas, procedimentos e tecnologias projetadas para proteger sistemas de computadores, redes, dispositivos e dados contra ameaças cibernéticas, ataques maliciosos e atividades não autorizadas. Vejamos o que prevê o artigo 5º, inciso XII da Constituição Federal de 1988:

> É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

O Artigo 5º, Inciso XII da Constituição Federal de 1988, desempenha um papel crucial na proteção da privacidade e liberdade individual dos cidadãos brasileiros. Ao garantir o sigilo das comunicações, estabelece-se um importante baluarte contra possíveis abusos estatais e violações dos direitos fundamentais. Esta disposição constitucional reflete os valores democráticos da sociedade brasileira e a necessidade de conciliar a segurança jurídica com a proteção dos direitos individuais em um mundo cada vez mais conectado e digitalizado.

Trata-se de uma disciplina multidisciplinar que abrange aspectos técnicos, legais e organizacionais, visando garantir a confidencialidade, integridade e disponibilidade das informações e recursos digitais de uma organização ou indivíduo.

Nesse sentido é importante a análise da jurisprudência que está descrita no Anexo A, que condena os réus pela prática de estelionato, com aumento da reincidência dos citados e ainda cita que na investigação teve quebra de sigilo

telefónico, que neste caso pode ser utilizado os dados e informações pessoais do indivíduo.

6.1 ESTRATÉGIAS DE CIBERSEGURANÇA PARA PREVENIR CRIMES VIRTUAIS.

As estratégias de cibersegurança desempenham um papel fundamental na prevenção de crimes virtuais. Essas estratégias incluem a implementação de sistemas de segurança robustos, como firewalls, antivírus e sistemas de detecção de intrusão, além de práticas de segurança de dados, como a criptografia e o monitoramento constante de atividades suspeitas.

Como já citado anteriormente a Convenção de Budapeste é de extrema importante para a cibersegurança, que conta com diversos países, estão entre eles, de acordo com o Roteiro de Atuação: Crimes Cibernéticos do MPF (2016):

> Atualmente a Convenção Internacional sobre Cibercrime conta com 22 signatários. Os países que assinaram o tratado são: Albânia, Armênia, Bósnia e Herzegovina, Bulgária, Chipre, Croácia, Dinamarca, Eslováquia, Eslovênia, Estados Unidos da América, Estônia, Finlândia, França, Hungria, Islândia, Letônia, Lituânia, Macedônia, Noruega, Países Baixos, Romênia e Ucrânia.

Ademais, a menção dos signatários da Convenção Internacional sobre Cibercrime no Roteiro de Atuação: Crimes Cibernéticos do MPF destaca a importância da cooperação internacional e da adoção de medidas conjuntas para combater eficazmente os crimes cibernéticos em escala global. Essa referência demonstra o compromisso do Brasil em contribuir para um ambiente digital mais seguro e protegido, alinhado aos esforços internacionais nesse sentido.

As empresas, como detentoras de dados sensíveis e infraestruturas digitais, têm a responsabilidade primária de implementar medidas robustas de segurança cibernética para proteger suas informações e sistemas contra ameaças virtuais. Isso inclui a adoção de políticas de segurança, criptografia de dados, autenticação, monitoramento proativo de redes e investimentos em treinamento e conscientização dos funcionários. Além disso, as empresas devem estar em conformidade com regulamentações de privacidade de dados e notificar as autoridades e partes interessadas em caso de violação de dados. Nesse contexto, Giacchetta (2015, online) diz:

> A Conforme previsto de forma clara pelo artigo 10, § 3º, a exceção é aplicável estritamente a dados que informem “qualificação pessoal, filiação e

> endereço". Requisições de autoridades administrativas visando o fornecimento de dados que não se enquadrem nos conceitos previstos extrapolam os limites da exceção e caracterizam abuso de poder. É o caso, por exemplo, de requisições que objetivem o fornecimento de telefone, e-mail e endereços de IP (Internet Protocol), ainda que sejam tais dados coletados no momento do cadastro no serviço.

Contudo, os indivíduos também têm um papel fundamental na proteção contra crimes cibernéticos. Devem adotar práticas de segurança digital em suas atividades online, como o uso de senhas fortes e únicas, a instalação regular de atualizações de software, a verificação de fontes de e-mails e a navegação segura na internet.

É importante ressaltar que a segurança cibernética é uma responsabilidade compartilhada entre empresas, governos e cidadãos. A colaboração e a cooperação entre essas partes são essenciais para enfrentar as ameaças cibernéticas de forma eficaz.

6.2 PROGRAMAS DE CONSCIENTIZAÇÃO E EDUCAÇÃO EM SEGURANÇA CIBERNÉTICA.

Ao longo dos anos, a legislação tem desempenhado um papel crucial na promoção da conscientização sobre cibersegurança e na prevenção de crimes virtuais. Através da promulgação de leis e regulamentos relacionados à proteção de dados, segurança cibernética e responsabilidade digital, os governos têm buscado educar indivíduos, empresas e instituições sobre os riscos associados à utilização da tecnologia e à presença online.

Além disso, as leis têm estabelecido diretrizes e padrões para a proteção de informações pessoais e confidenciais, incentivando a implementação de medidas de segurança, como criptografia, autenticação multifator e políticas de privacidade robustas. Por meio de campanhas de conscientização, programas de educação digital, workshops, materiais educativos e iniciativas de cibersegurança, a legislação tem contribuído para aumentar a compreensão dos cidadãos e organizações sobre os perigos do cibercrime e as melhores práticas para se proteger online.

No entanto, é importante reconhecer que os desafios em matéria de segurança cibernética continuam a evoluir, e que a legislação deve acompanhar essas mudanças para garantir uma proteção eficaz contra as ameaças virtuais em constante

mutação. Os indivíduos também devem estar cientes dos seus direitos e responsabilidades em relação à proteção de dados pessoais e à privacidade online.

CONCLUSÃO

Ao longo deste trabalho, foi possível realizar uma análise abrangente e detalhada sobre o tema dos Crimes Virtuais: A Evolução e a Análise da Aplicação do Direito. Através da investigação cuidadosa da história, evolução e características desses delitos, foi possível compreender a complexidade e os desafios enfrentados pelo sistema jurídico na sua abordagem.

Ficou evidente que os crimes virtuais representam uma ameaça significativa para a sociedade contemporânea, com impactos que vão desde prejuízos financeiros e danos à reputação até questões relacionadas à privacidade, segurança e direitos individuais. A natureza global e dinâmica desses delitos demanda respostas rápidas e eficazes por parte das autoridades e do sistema jurídico.

No entanto, também foi possível identificar avanços significativos na legislação e nas estratégias de aplicação da lei voltadas para o combate aos crimes virtuais. A criação de leis específicas, o fortalecimento da cooperação internacional e o investimento em tecnologias de segurança cibernética são exemplos de medidas adotadas para enfrentar essa problemática de forma mais eficiente.

É fundamental ressaltar que o enfrentamento dos crimes virtuais requer não apenas uma resposta repressiva, mas também a promoção de ações preventivas e educativas. A conscientização da sociedade sobre os riscos e as melhores práticas de segurança cibernética é essencial para mitigar essas ameaças e proteger os indivíduos e as organizações contra os ataques virtuais.

Portanto, diante da crescente sofisticação e diversificação dos crimes virtuais, é imperativo que o sistema jurídico continue a evoluir e se adaptar para enfrentar esses desafios em constante mutação. Somente através de uma abordagem abrangente e colaborativa, envolvendo governos, empresas, organizações da sociedade civil e cidadãos, será possível garantir um ambiente digital seguro e protegido para todos.

REFERÊNCIAS

ARBEX, Thais. **Lava Jato formalizou cooperação internacional um ano após leniência com Odebrecht, aponta documento de ministério**. CNN Brasil, Brasília. 2023. Disponível em: https://www.cnnbrasil.com.br/politica/lava-jato-formalizou-cooperacao-internacional-um-ano-apos-leniencia-com-odebrecht-aponta-documento-de-ministerio/ . Acesso em: 29 de novembro de 2023.

Barreto, A. G., Kufa, K., & Silva, M. M. (2022). **Cibercrimes e seus reflexos no direito brasileiro.** JusPodivm

BOM, N. E SCOTT, D. (2019). **O lado negro da revolução digital: do ciberespaço ao cibercrime**. Rowman e Littlefield.

Bomfati, C. A., & Junior, A. K. (2020). **Crimes cibernéticos: Aspectos Jurídicos.** InterSaberes.

BARRETO, Alessandro Gonçalves, BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet.** 1 Ed., São Paulo: Brasport, 2016.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 29 de fevereiro de 2024.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm. Acesso em: 15 de novembro de 2023.

BRASIL. Decreto nº 5.015, de 12 de março de 2004. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional. Brasília, 2004. Disponível:https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm Acesso em: 29 de fevereiro de 2024

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. **Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em**

Budapeste, em 23 de novembro de 2001. Brasília, DF, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm Acesso em: 29 de fevereiro de 2024.

BRASIL. Lei nº 11.343, de 23 de agosto de 2006. **Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências.** Brasília, DF, 2006. Disponível: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm Acesso: 29 de fevereiro de 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências**. Brasília, DF: Palácio do Planalto, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm#art4. Acesso em: 15 de novembro de 2023.

BRASIL. Lei nº 12.850, de 2 agosto de 2013. **Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências.** Brasília, DF, 2013. Disponível: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm Acesso: 29 de fevereiro de 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília, DF: Palácio do Planalto, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 de novembro de 2023.

BRASIL. Lei nº 13.441, de 8 de maio de 2017. **Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade**

sexual de criança e de adolescente. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm Acesso em: 29 de fevereiro de 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** (Redação dada pela Lei nº 13.853, de 2019). Disponivel em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 de novembro de 2023.

BRENNER, SW (2012). **Crime cibernético e a lei: desafios, questões e resultados**. Praeger.

BRITZ, Marjie T. **Computer forensics and cybercrime: an introduction**. New Jersey: Pretice Hall, 2009, p. 4.

CALIXTO, Tharynne Marcela Barbosa; FACURI, Antônio Carlos Gomes; TELES, Fernando Hugo Miranda. **As relações de cooperação jurídica internacional no combate às práticas de cibercrimes**. Revista do Ministério Público Militar, [S. l.], v. 50, n. 39, p. 235–244, 2023. Disponível em: https://revista.mpm.mp.br/rmpm/article/view/148. Acesso em: 8 mar. 2024.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Âmbito Jurídico. 2012. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/>. Acesso em: 08 de março de 2024.

DINO. **Brasil vive aumento no número de crimes cibernéticos.** Disponível em: https://valor.globo.com/patrocinado/dino/noticia/2023/08/01/brasil-vive-aumento-no-numero-de-crimes-ciberneticos.ghtml Acesso em 29 de fevereiro de 2024.

EUROPA. Reforma da cibersegurança na Europa. Disponível em: http://www.consilium.europa.eu/pt/policies/cyber-security/ Acesso em: 29 de fevereiro de 2024.

FINKLEA, KM (2019). **Crime cibernético: uma visão geral do Estatuto Federal de Fraude e Abuso de Computadores e das Leis Penais Federais Relacionadas.** Serviço de Pesquisa do Congresso.

GOIÁS. Tribunal de Justiça. **Apelação Criminal**. Processo 5344968-06.2022.8.09.0051 da 2ª Câmara Criminal. Relator Desembargador Edison Miguel da Silva Junior. Disponível em: 5344968-06.2022.8.09.0051. Acesso em: 29 de fevereiro de 2024.

GRAELL, F. e VINCAX, M. **Lei Carolina Dieckmann completa 10 anos como marco no combate a crimes cibernéticos**. G1 – GLOBO, [S.l.]. 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/12/02/lei-carolina-dieckmann-completa-10-anos-como-marco-no-combate-a-crimes-ciberneticos.ghtml . Acesso em: 29 de novembro de 2023.

HOLT, TJ E BOSSLER, AM (2016). **Crimes Cibernéticos em Andamento: Teoria e Prevenção de Delitos Habilitados pela Tecnologia.** Crime e Delinquência, 62 (2), 161-161.

Jorge, H. V., & Wendy, E. (2017). **Crimes cibernéticos: Ameaças e procedimentos de investigação - 2ª Edição.** Brasport.

KERR, OS (2012). **Lei de Crimes Informáticos.** Publicação Acadêmica Ocidental.

Ministério Público Federal. **Roteiro de Atuação – Crimes Cibernéticos.** Brasília/DF, 2016. Disponível em: https://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Biblioteca_Virtual/Livros_Digitais/MPF%203186_Crimes_Ciberneticos_2016.pdf Acesso em: 29 de fevereiro de 2024

PAREDE, D. (2015). ***Crimes Cibernéticos.***

PAREDE, D.S. (2015). **Crime Cibernético: A Transformação do Crime na Era da Informação**. Wiley.

PINHEIRO, Patrícia Peck. Direito digital. 5. Ed. São Paulo: Saraiva, 2013.

ROHR, Altieres. **Megavazamentos de dados expõem informações de 223 milhões de números de CPF**. G1 GLOBO, [S.l.]. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml . Acesso em: 29 de novembro de 2023.

SAIGG, Mahomed. **Hacker conta em depoimento como chegou a arquivos de Deltan Dallagnol e os repassou a Glenn Greenwald e diz que não recebeu dinheiro pelo material**. G1 GLOBO, Brasília. 2019. Disponível em: https://g1.globo.com/politica/noticia/2019/07/26/hacker-diz-em-depoimento-como-chegou-aos-arquivos-de-deltan-e-que-nao-recebeu-dinheiro-pelo-material.ghtml . Acesso em: 29 de novembro de 2023.

TORRES, Cláudio. **A bíblia do marketing digital: tudo o que você queria saber sobre o marketing e a publicidade na internet e não tinha a quem perguntar**. São Paulo: Novatec, 2009. P. 24

UCHINAKA, Fabiana. **WannaCry: após um ano, ainda não brecaram o maior ciberataque da história**. Tilt uol, São Paulo. 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/05/05/wannacry-apos-um-ano-ainda-nao-brecaram-o-maior-ciberataque-da-historia.htm . Acesso em: 29 de novembro de 2023.

YAR, M. (2013). **Cibercrime e Sociedade.** Publicações Sábias.

ANEXO A – JURISPRUDÊNCIA REFERENTE À PRÁTICA DE CRIME DE ESTELIONATO

GOIÁS. TRIBUNAL DE JUSTIÇA DO ESTADO DE GOIÁS. APELAÇÃO CRIMINAL 5344968-06.2022.8.09.0051. APELANTES: WENDEL JUNIO MIRANDA CARVALHO LEONARDO LOPES DOS ANJOS VITOR HUGO MARTINS CRISTINO JOÃO HENRIQUE PIRES DE CAMARGO SENHORINHO YAN DA SILVA MELO. APELADO: MINISTÉRIO PÚBLICO. RELATOR: DESEMBARGADOR EDISON MIGUEL DA SILVA JUNIOR. 21 DE FEVEREIRO DE 2024. Relatório Organização criminosa e estelionatos via plataforma virtual. Condenações. Penas somadas: 13 anos e 05 meses

de reclusão, no regime inicial fechado, e 102 dias-multa (Wendel); de 07 anos e 05 meses de reclusão, no regime inicial fechado, e 27 dias-multa (João Henrique); 07 anos e 02 meses de reclusão, no regime inicial fechado, e 26 dias-multa (Vitor Hugo e Yan), todos no regime inicial fechado; 05 anos e 07 meses de reclusão, no regime inicial semiaberto, e 31 dias-multa, no regime semiaberto (Leonardo). Apelos da defesa arguindo nulidades: ilegalidade da abordagem e busca veicular e da quebra de sigilo de dados telefônicos. Sustentou absolvição; redimensionamento das penas; e recurso em liberdade. (1) A sentença rechaçou, pontualmente, todas as teses de nulidades reiteradas no presente recurso, ressaltando que o contexto dos fatos apresentados nos autos, em que o cenário anterior à abordagem permitia concluir pela ocorrência de conduta ilícita, revelando-se legítima a abordagem e busca veicular e com a apreensão do numerário em espécie, em tese, sem origem lícita, a carteira de identidade de terceiro e os três aparelhos celulares, além das informações que o réu estava envolvido em estelionatos eletrônicos e acompanhada a representação por documentos relacionados ao inquérito instaurado, onde constava indícios de golpes praticados com o uso de telefone, justificando, assim, o deferimento da quebra de sigilo de dados dos aparelhos. (2) Os depoimentos testemunhais, a quebra de sigilo de armazenamento de dados e demais provas colhidas comprovam a existência de uma organização criminosa destinada à prática de diversos estelionatos, por meio de plataforma virtual, onde os réus utilizavam uma ferramenta digital, por meio da qual vítimas de vários Estados da Federação foram ludibriadas por meio do WhatsApp, por pessoas que se passavam por seus parentes, ficando constatado pelos diálogos o vínculo associativo estável. Da mesma forma a prova dos autos é suficiente para a condenação dos réus pelos crimes de estelionato. (3) As penas não merecem reparos, porquanto houve fundamentação idônea das circunstâncias judiciais, os patamares de aumento pela agravante da reincidência foram justos e necessários. (4) Presentes os requisitos legais, mantém-se a prisão cautelar do agente. (5) Apelos conhecidos e desprovidos.