PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

A ATUAÇÃO DO DIREITO PENAL NO COMBATE AOS CIBERCRIMES:

PERSPECTIVAS PARA A EFETIVIDADE DA JUSTIÇA DIGITAL

ORIENTANDA – GEOVANNA SANTOS MARTINS

ORIENTADORA – PROFA. DRA. FÁTIMA DE PAULA FERREIRA

GOIÂNIA-GO

2024/1

GEOVANNA SANTOS MARTINS

A ATUAÇÃO DO DIREITO PENAL NO COMBATE AOS CIBERCRIMES:

PERSPECTIVAS PARA A EFETIVIDADE DA JUSTIÇA DIGITAL

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 (PUCGOIÁS).
Orientadora – Dra. Fátima de Paula Ferreira.

GOIÂNIA-GO

2024/1

GEOVANNA SANTOS MARTINS

A ATUAÇÃO DO DIREITO PENAL NO COMBATE AOS CIBERCRIMES:

PERSPECTIVAS PARA A EFETIVIDADE DA JUSTIÇA DIGITAL

Data da Defesa: 18 de maio de 2024

BANCA EXAMINADORA

_____

Orientadora: Profa.: Dra. Fátima de Paula Ferreira Nota

_____

Examinador Convidado: Prof. Ms. Eurípedes Clementino Ribeiro Júnior Nota

SUMÁRIO

A ATUAÇÃO DO DIREITO PENAL NO COMBATE AOS CIBERCRIMES:

PERSPECTIVAS PARA A EFETIVIDADE DA JUSTIÇA DIGITAL

Geovanna Santos Martins[1]

RESUMO

Este artigo tem como método científico hipotético-dedutivo e terá como objetivo conceituar e introduzir o que são os crimes cibernéticos, além de mostrar como o Direito Penal legisla sobre certos crimes que migraram do ambiente real para o ambiente virtual. No entanto, também é dissertado sobre a segurança cibernética, algo de extrema relevância para que tenhamos um ambiente virtual seguro. Sendo assim, tem como conclusão que a partir dos questionamentos levantados na introdução pode-se concluir que os crimes normais e os cibercrimes diferem em vários aspectos devido à sua natureza e à maneira como são cometidos.

Palavras-chave: Crimes cibernéticos. Ambiente Virtual. Direito Digital.

ABSTRACT

This article employs the hypothetico-deductive scientific method and aims to conceptualize and introduce what cybercrimes are, as well as to demonstrate how Criminal Law legislates on certain crimes that have migrated from the real to the virtual environment. Additionally, it discusses cyber security, something of extreme relevance for ensuring a safe virtual environment. Therefore, it concludes that from the questions raised in the introduction, it can be concluded that normal crimes and cybercrimes differ in various aspects due to their nature and the way they are committed.

Keywords: Cybercrimes. Virtual environment. Digital Law.

[1] Acadêmica do curso de Direito da Pontifícia Universidade Católica de Goiás (PUC GO), e-mail: santosmartinsgeovanna@gmail.com

INTRODUÇÃO

A presente pesquisa tem como objetivo primordial examinar a abordagem do Direito Penal no combate aos Cibercrimes, também conhecidos como crimes cibernéticos. O foco está em analisar os obstáculos enfrentados pela área penal em combater a cibercriminologia, fazendo com que haja a concretização da justiça digital.

A escolha deste tema foi devido a constante evolução da internet. Nos últimos anos, temos testemunhado a ocorrência de eventos marcantes que provocaram a migração da maioria dos trabalhos e atividades para o *online*. Como consequência, os delitos penais também migraram para o cenário digital. Sendo assim, o tema foi escolhido quando eu presenciei acontecimentos e notícias de fraudes pelo *WhatsApp*, invasões de contas bancárias, vazamento de dados pessoais, clonagem de cartões, difamação de teor racial, entre outras transgressões.

Estes crimes podem causar danos significativos a indivíduos, empresas e organizações, muitas vezes transcendo fronteiras nacionais, o que torna o seu combate um desafio global. E ao decorrer desta pesquisa veremos os desafios e perspectivas da área penal em fazer com que haja a efetividade da justiça no mundo cibernético.

Dessa maneira, é evidente que a criminalidade não está mais restrita às ruas, mas se amplia ao ambiente digital. Por isto o tema abordado é de extrema relevância social, pois além de abordar as problemáticas jurídicas e tudo o que ela envolve, também será um tema que debate de uma forma que alerta a sociedade sobre esta “nova” modalidade de prática de infrações penais, com a qual o Direito Penal lida e combate.

Este presente trabalho tem por objetivo geral mostrar a importância do Direito Penal no Combate aos Cibercrimes. E por objetivos específicos introduzir e conceituar os Cibercrimes, dando enfoque nas legislações presentes no nosso Código Penal, explicar como o Direito Penal atua no Combate aos Cibercrimes e informar os tipos de crimes e trazer um caso relacionado com o tema.

Os principais questionamentos que despertaram o interesse para o desenvolvimento do presente artigo estão relacionados em compreender como os crimes cibernéticos se diferenciam dos crimes convencionais, bem como elencar quais são os principais desafios legais e técnicos associados à investigação e à coleta de evidências em casos de crimes digitais, assim como refletir acerca de como o

sistema legal está se adaptando para enfrentar os desafios dos crimes digitais e, ainda, compreender como o Direito Penal aborda os crimes cibernéticos, considerando que estes podem ocorrer em qualquer lugar e serem cometidos por qualquer indivíduo.

Assim, o presente trabalho acadêmico faz-se realizado a partir o método científico hipotético-dedutivo, partindo de ideias gerais para conclusões específicas, formulando hipóteses sobre as dificuldades abordadas. Ainda, utilizou-se de pesquisas bibliográficas e documentais, recorrendo a diversas fontes para introduzir o assunto e encontrar soluções, fazendo comparações e usando conceitos já existentes relacionados à doutrinas e jurisprudências das áreas do Direito Penal e Direito Digital.

Destaca-se, por demais, que este artigo científico possui, ainda, o objetivo de investigar a eficácia da atuação do Direito Penal no combate aos cibercrimes e discutir as implicações dos resultados para a melhoria da efetividade da justiça digital.

1 DO DIREITO DIGITAL

No contexto digital, é crucial que a legislação esteja sintonizada com os avanços sociais e tecnológicos, buscando regularizar as emergentes dinâmicas relacionais nesse ambiente. Apesar dos inúmeros ganhos proporcionados pela tecnologia, o espaço virtual, por outro lado, tem se transformado em cenário propício para a perpetração de novos crimes, sobretudo devido à possibilidade de criminosos se ocultarem no anonimato na tentativa de assegurar a impunidade de suas ações. Nesse sentido, é essencial que o ordenamento jurídico se adeque a essas mudanças, promovendo uma resposta eficaz diante das práticas delituosas no mundo digital.

E assim, devido ao desenvolvimento da tecnologia e da interação online surgiu a indispensabilidade de normas que regulamentam as relações entre os usuários e adeptos. Desse modo o Direito Digital chegou para regulamentar as relações entre a disciplina do Direito e a informática, assim aplicando novas tecnologias.

O direito digital, conhecido também como direito da informática ou direito cibernético, é uma disciplina jurídica que se dedica a questões legais no contexto da tecnologia da informação, internet, computação e comunicação digital. Abrange uma

ampla gama de temas, que incluem desde questões relacionadas à propriedade intelectual até aspectos de privacidade, segurança cibernética, responsabilidade legal e regulamentações da rede. Esse campo legal enfrenta os desafios e complexidades que emergem devido à rápida evolução da tecnologia digital e da sociedade da informação.

Patrícia Peck reflete que o Direito Digital

> consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc. (2021, p. 49)

Desse modo, os crimes cibernéticos se encontram na área criminal que é uma das áreas que o Direito Digital atua.

1.1. DO CONCEITO DE CIBERCRIME

O cibercrime, também conhecido como crime cibernético ou crime digital, refere-se a atividades criminosas que envolvem o uso de computadores e redes de computadores. Estas atividades podem incluir ataques a sistemas computacionais, roubo de dados pessoais e financeiros, entre outros. A história do cibercrime surge no início da era da computação, com o aumento da tecnologia e da conectividade global.

Segundo Guimarães e Neto, crime informático significa "qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados" (2003, p. 04).

Os crimes virtuais surgiram em paralelo ao desenvolvimento da internet e têm evoluído ao longo dos anos, sempre com o objetivo de causar prejuízos a outros usuários. Também conhecidos como crimes eletrônicos ou cibernéticos, esses delitos são cometidos em um espaço fictício criado pela rede mundial de computadores, a Internet. Neles, o agente não precisa estar em um território físico específico para cometer o crime, e a vítima também não necessariamente precisa ser abordada fisicamente. (MIRANDA, 2013 *apud* LORENZO; SCARAVELLI, 2021, 04).

Fabrizio Rosa também conceitua o crime cibernético, sendo este

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou

> armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O "Crime de Informática" é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o "Crime de Informática" pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (ROSA, 2002, p. 53).

Ainda, sobre os delitos informáticos, é importante destacar que

> a denominação "delitos informáticos" alcança não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta sem imprescindível "conexão" à Rede Mundial de Computadores, ou qualquer outro ambiente telemático. Ou seja, uma fraude em que o computador é usado como instrumento do crime, fora da internet, também seria alcançada pelo que se denominou "delitos informáticos" (ROSSINI, 2004, p. 110).

Sendo assim, o crime cibernético não é somente aquele que é cometido no âmbito da internet, mas também é aquele que a conduta tenha relação com o sistema informáticos redes.

1.1.1 Da Segurança Cibernética

Ao decorrer que a sociedade se torna cada vez mais dependente de tecnologias da informação e comunicação e com a rápida expansão do ciberespaço, tanto empresas, organizações governamentais e indivíduos encaram uma crescente ameaça de ataques cibernéticos que acabam prejudicando financeiramente e moralmente. Devido a essa expansão do ciberespaço e o crescimento do acesso das redes veio a precisão de encontrar maneiras de tornar este espaço um lugar mais seguro e sem riscos.

No entanto o que pode ser um risco no ambiente digital, Sydow Spencer pondera que:

> Os riscos informáticos são aqueles que colocam em jogo a perda ou a diminuição desses novos valores informáticos que surgem: a tranquilidade para navegar, a segurança para se fazer operações em plataformas digitais, o acesso à virtualidade propriamente dito, a integridade dos arquivos armazenados, a confiabilidade da nuvem, a não destruição da imagem virtual construída, a possibilidade de se acessar os sistemas contratados, a garantia de fornecimento de serviço digital de provimento de acessos, e assim por diante (SYDOW, 2023 p. 43).

A segurança cibernética diz respeito a prática de garantir a segurança nos sistemas de redes, computadores e dados contra ameaças cibernéticas. Sendo assim, tem como finalidade assegurar a privacidade das informações, assim protegendo os sistemas contra danos das atividades maliciosas no âmbito digital.

Logo o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República aborda no Glossário de Segurança da Informação as ações que são destinadas a segurança cibernética:

> A segurança cibernética é definida como “ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis” (GSI/PR).

Contudo, a concretização real da segurança cibernética é um empecilho contínuo que necessita de investimentos do governo e requer atenção do sistema jurídico brasileiro. Ao decorrer que o Brasil avança na implementação dessas práticas, a capacidade do país em proteger seus ativos digitais e infraestrutura crítica será crucial para garantir um ambiente digital seguro e resiliente.

2 DA ATUAÇÃO DO DIREITO PENAL NO COMBATE AOS CIBERCRIMES

A crescente interconexão digital trouxe inúmeras vantagens para a sociedade moderna, mas também deu origem a uma nova categoria de crimes: os cibercrimes. Essas atividades ilícitas, perpetradas através da internet e de dispositivos eletrônicos, representam desafios únicos para a aplicação da lei, exigindo uma abordagem especializada por parte do sistema jurídico.

Nesse contexto, a atuação do Direito Penal no combate aos cibercrimes torna-se fundamental para proteger os indivíduos, as organizações e a infraestrutura digital contra ameaças virtuais. Dessa forma, há a extrema necessidade de explorar como o Direito Penal se adapta e evolui para lidar com os desafios apresentados pelos

cibercrimes, destacando tanto os avanços quanto as lacunas que ainda precisam ser preenchidas nesse campo dinâmico e em constante transformação.

2.1 DAS LEIS E REGULAMENTOS RELACIONADOS AOS CRIMES CIBERNETICOS

No Brasil, as leis e regulamentos relacionados aos crimes cibernéticos têm ganhado cada vez mais relevância diante do avanço da tecnologia e da crescente dependência da sociedade em relação à internet e aos dispositivos eletrônicos. Desde a promulgação do Marco Civil da Internet, em 2014, diversas medidas têm sido implementadas para combater e prevenir os delitos virtuais.

O Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, incluindo a proteção da privacidade e dos dados pessoais dos usuários. Além disso, o Código Penal Brasileiro tipifica uma série de condutas criminosas relacionadas à internet.

Outrora, Neves e Vancim refletem que

> Definida como “Constituição” da *Internet*, referido texto normativo veio a aprimorar e delimitar o uso da Internet no Brasil, de modo a conferir maior garantia dos direitos advindos da rede, bem assim, mais direitos e deveres aos usuários, como *novatio legis* especial de regulamentação detalhada e precisa dos direitos da *Internet*. (NEVES, VANCIM, 2015, p. 21).

Por seguinte, para Barreto Júnior e César, “o Marco Civil da Internet é uma resposta do Poder Legislativo brasileiro aos conflitos inerentes à sociabilidade humana, surgidos com a disseminação da sociedade da informação” (2017, p. 84).

Ainda, tem-se a Lei 12.737/2012 de Crimes Cibernéticos, conhecida como "Lei Carolina Dieckmann", tipifica delitos como a invasão de dispositivos informáticos, a divulgação de informações pessoais sem consentimento e a interrupção de serviços telemáticos.

O artigo154-A dispõe sobre a invasão de dispositivo informático:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita;
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações

> sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Assim sendo, o artigo supramencionado estabelece que acessar indevidamente dispositivos eletrônicos alheios, como computadores, *smartphones* e *tablets*, com o intuito de obter, adulterar ou destruir dados sem autorização do titular, configura uma conduta criminosa.

Nesse sentido, há a reflexão de que esta lei visa a proteger a integridade e a privacidade das informações pessoais armazenadas nos dispositivos eletrônicos, estabelecendo penas para quem cometer esse tipo de delito, que podem variar de acordo com a gravidade da invasão e o prejuízo causado à vítima.

Em outro viés, a legislação brasileira sobre ação penal e crimes contra a administração pública e serviços de utilidade pública apresenta nuances importantes para o devido processo legal e a preservação da ordem social.

O artigo 154-B do Código Penal estabelece que nos casos de crimes definidos no artigo 154-A, a ação penal somente se procede mediante representação, a menos que o delito seja cometido contra a administração pública direta ou indireta ou empresas concessionárias de serviços públicos:

> **Ação penal**
> 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.”

Além disso, recentes alterações no Código Penal, promovidas pelo Decreto-Lei nº 2.848, de 7 de dezembro de 1940, trazem novos dispositivos para coibir a interrupção ou perturbação de serviços telegráficos, telefônicos, informáticos, telemáticos ou de informação de utilidade pública, bem como para criminalizar a falsificação de documentos particulares, incluindo cartões de crédito ou débito:

> Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

> **“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública”**
> Art. 266.. .....
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)
> **“Falsificação de documento particular**
> Art. 298.. .....
> **Falsificação de cartão**
> Parágrafo único. Para fins do disposto no caput , equipara-se a documento particular o cartão de crédito ou débito.” (NR)

Por demais das leis referidas acima, o Brasil também é signatário de tratados internacionais que visam combater os crimes cibernéticos. A Convenção de Budapeste busca, por meio do Conselho da Europa e os países que a assinam, estabelecer uma maior integração entre eles. Seu propósito é reconhecer a primazia de uma política criminal comum, com o objetivo de proteger a sociedade contra os delitos cibernéticos, promovendo a colaboração internacional.

Em 12 de abril 2023, o Decreto Federal N. 11.491 foi promulgado, o qual traz novas medidas a serem adotadas e novas definições sobre os crimes cibernéticos. Os crimes citados neste novo Decreto, à luz da Convenção de Budapeste, se encaixam como crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador**,** violação de direitos autorais e de direitos correlatos, pornografia infantil, fraude informática, falsificação informática, uso indevido de aparelhagem, interferência em sistema, violação de dados, interceptação ilícita e acesso ilegal.

Todavia, à par destes avanços legislativos, tais quais os decretos federais de combate aos crimes cibernéticos, ainda há desafios a serem enfrentados, como a necessidade de atualização constante das leis para acompanhar o desenvolvimento tecnológico, a falta de estrutura adequada para investigação e punição dos criminosos cibernéticos e a conscientização da população sobre os riscos e medidas de segurança na internet.

Portanto, a eficácia no combate aos crimes cibernéticos no Brasil depende não apenas da existência de leis e regulamentos adequados, mas também da colaboração entre governo, empresas e sociedade civil, bem como do fortalecimento das instituições responsáveis pela aplicação da lei e pela proteção dos cidadãos no ambiente digital.

2.1.1 Da Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD), regulamenta o tratamento de dados pessoais por empresas e organizações. Ela estabelece regras sobre a coleta, armazenamento, processamento e compartilhamento de informações pessoais, visando proteger a privacidade e os direitos dos cidadãos. A LGPD também define obrigações para as empresas em relação à segurança dos dados e estabelece direitos dos titulares das informações, como o acesso aos seus dados e a possibilidade de solicitar correções ou exclusões. A lei prevê penalidades para o descumprimento das suas disposições, incluindo multas e sanções administrativas.

O Artigo 2º da legislação sobre proteção de dados pessoais delineia os pilares fundamentais que sustentam toda a estrutura normativa no campo cibernético:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Esses fundamentos estabelecem equidade entre a evolução tecnológica, os avanços e os direitos individuais. Desde o respeito à privacidade até a promoção dos direitos humanos, cada elemento desse conjunto reflete a complexidade e a importância da proteção dos dados pessoais em uma sociedade moderna e interconectada.

2.2 Do Papel do Direito Penal da Prevenção e Repreensão

O papel do Direito Penal na prevenção e repressão dos crimes cibernéticos é crucial em uma era onde a tecnologia permeia todos os aspectos de nossas vidas. Com o avanço da internet e das tecnologias digitais, surgiram novas formas de crimes, que muitas vezes ultrapassam fronteiras físicas e desafiam os sistemas jurídicos tradicionais. Nesse contexto, o Direito Penal desempenha um papel fundamental na proteção dos indivíduos e da sociedade contra essas ameaças virtuais.

A prevenção dos crimes cibernéticos começa com a definição clara de leis que abordam especificamente essas questões. O Direito Penal deve acompanhar de

perto o desenvolvimento tecnológico para garantir que as leis estejam atualizadas e sejam eficazes na prevenção e repressão desses delitos. Além disso, é essencial que haja cooperação internacional para combater os crimes cibernéticos, dada sua natureza transnacional.

Apesar da reflexão no ponto de vista dos textos legais, decreto específico e a Convenção de Budapeste, o Brasil sofre inúmeras críticas no que se refere à sua legislação, de modo geral, haja vista o atual cenário do avanço era digital, ao qual a principal crítica entorna ao fato “não haver uma legislação específica à respeito de crimes virtuais ou cibernéticos, ou mesmo com a legislação existente, ainda ser um país que sofre constantemente com a prática de crimes virtuais” (BARBOSA, 2020, p.18).

As punições previstas pelo Direito Penal devem ser proporcionais à gravidade do crime e capazes de desencorajar os infratores. Isso inclui penas que vão desde multas até prisão, dependendo da gravidade do delito e do dano causado. No entanto, é importante que o Direito Penal também busque formas de reabilitação para os infratores, especialmente considerando a rápida evolução do cenário tecnológico, que pode tornar alguns crimes obsoletos.

Além da repressão, o Direito Penal também desempenha um papel na prevenção dos crimes cibernéticos por meio da educação e conscientização. É essencial que os usuários da internet compreendam os riscos associados ao uso da tecnologia e saibam como proteger suas informações pessoais e evitar serem vítimas de crimes virtuais. As campanhas de conscientização podem ajudar a reduzir a vulnerabilidade das pessoas aos ataques cibernéticos.

Outro aspecto importante é a investigação e o julgamento eficazes dos crimes cibernéticos. As autoridades policiais e judiciais devem estar devidamente capacitadas e equipadas para lidar com a complexidade desses casos, incluindo a coleta de evidências digitais e a colaboração com especialistas em tecnologia da informação. O uso de tecnologias forenses é essencial para garantir a integridade das investigações e a condenação dos culpados.

Em síntese, o Direito Penal desempenha um papel fundamental na prevenção e repressão dos crimes cibernéticos, garantindo a segurança e proteção dos indivíduos e da sociedade em um mundo cada vez mais digitalizado, pois é através de leis claras, punições proporcionais, educação e conscientização, investigação eficaz e regulação adequada, que o Direito Penal pode auxiliar no enfrentamento dos

desafios trazidos pela era digital e garantir um ambiente online mais seguro e confiável para todos.

3 DOS TIPOS CRIMINAIS E CASOS NOTÁVEIS

Na era digital em que vivemos, os crimes cibernéticos emergem como uma ameaça crescente e complexa, desafiando não apenas a segurança de indivíduos, mas também a estabilidade de empresas e até mesmo de nações inteiras. Estes crimes, que abrangem uma ampla gama de atividades ilícitas realizadas através da internet e de dispositivos eletrônicos, representam uma nova fronteira para a aplicação da lei e para a proteção dos dados pessoais e sensíveis.

Dessa forma, existem variados tipos de atos ilícitos que visam obter vantagens indevidas por meio das ações digitais, bem como ameaçam a segurança humana ou, simplesmente, são cometidos para ferirem a dignidade humana e criarem mazelas, tanto social quanto particularmente, às vidas das vítimas.

3.1 DA FRAUDE *ONLINE*, DO *PHISHING* E DO *BULLYNG* CIBERNÉTICO

A fraude *online* é um dos crimes cibernéticos mais persistente no mundo digital atual, representando um perigo invisível que pode afetar qualquer pessoa conectada à internet. Por meio de métodos sofisticados, os fraudadores exploram vulnerabilidades nos sistemas digitais para obter ganhos financeiros ilícitos.

Já o *phishing* é uma das formas mais comuns e perigosas de fraude online, esta prática criminosa que visa ludibriar indivíduos para que divulguem informações confidenciais, como senhas e números de cartões de crédito.

Analogamente a uma pescaria, existem várias formas de fisgar uma vítima, porém uma tática específica de *phishing* é mais prevalente. Geralmente, as vítimas recebem um e-mail ou mensagem de texto que se faz passar (ou "finge ser") por alguém ou alguma instituição de confiança, como um colega de trabalho, um banco ou uma entidade governamental.

Nesse modo, ao abrir o e-mail ou texto, são confrontadas com uma mensagem alarmante que as instiga a deixar de lado o bom senso, induzindo-as ao medo. Essa

mensagem geralmente pressiona a vítima a acessar um site e realizar uma ação imediata, sob ameaça de enfrentar consequências adversas.

As consequências do *phishing* podem ser inúmeras, resultando em roubo de identidade, perda financeira e comprometimento da segurança online. Para se proteger contra esta modalidade de fraude, é essencial que os usuários estejam sempre vigilantes e verifiquem cuidadosamente a autenticidade de mensagens e sites antes de compartilhar qualquer informação pessoal.

O *cyberbullying* ou *bullying* cibernético é um crime perpetrado através de plataformas virtuais como redes sociais, aplicativos de mensagens e fóruns online, caracterizando-se pela repetição de comportamentos agressivos por parte de um ou mais agressores.

Além de envolver ofensas, difamação e divulgação de informações ou imagens pessoais da vítima, esse fenômeno muitas vezes surge como uma extensão do bullying tradicional, no qual ameaças e agressões são perpetradas pessoalmente. Como consequência, o *cyberbullying* gera impactos graves na saúde emocional e bem-estar psicológico das vítimas, causando ansiedade, depressão e até mesmo levando a casos extremos como o suicídio.

Assim, reflete-se que, para o combate deste crime cibernético, é crucial que sejam adotadas medidas de prevenção e apoio às vítimas que promovam uma cultura online de respeito, empatia e apoio mútuo.

3.2 DO CASO CAROLINA DIECKMANN

Tangente à casos que geraram grande repercussão no Brasil e solidificaram a reflexão sobre os perigos dos crimes cibernéticos, tem-se o caso Carolina Dieckmann, ocorrido em 2012, que trouxe à tona questões cruciais sobre a segurança digital e a privacidade na era da internet.

No caso em questão, a atriz brasileira Carolina Dieckmann teve seu computador pessoal invadido, resultando no vazamento de fotos íntimas. Esse incidente não apenas expôs a vulnerabilidade de figuras públicas, mas também levantou debates sobre os limites da privacidade online e a necessidade de leis mais rígidas para proteger os dados pessoais.

A repercussão do caso evidenciou a urgência de medidas preventivas tanto no âmbito individual, como o fortalecimento de práticas de segurança digital, quanto

no âmbito legal, com a implementação de políticas que garantam a proteção da privacidade de todos os usuários da internet. E assim foi criada a Lei 12.737/2012, que veio deste fato ocorrido com a atriz.

Neste viés, analisa-se que a história de Carolina Dieckmann serviu como um alerta para a importância da conscientização sobre os riscos cibernéticos e da adoção de medidas proativas para proteger a privacidade e a segurança online.

3.2.1 Da importância da Repercussão Legal e Midiática dos Cibercrimes

A importância da repercussão legal e midiática dos cibercrimes não pode ser subestimada, pois esses incidentes têm um impacto significativo em diversos aspectos da sociedade contemporânea.

Primeiramente, a ampla divulgação desses crimes na mídia é crucial para conscientizar o público sobre os riscos e as consequências da atividade criminosa online. Isso ajuda a educar os usuários sobre a importância da segurança cibernética e incentiva a adoção de medidas preventivas para proteger seus dados pessoais e informações sensíveis.

Além disso, a repercussão midiática dos cibercrimes muitas vezes pressiona as autoridades a agirem com mais vigor na investigação e punição dos criminosos cibernéticos. A visibilidade desses casos pode aumentar a pressão pública sobre os órgãos responsáveis pela aplicação da lei, levando a uma resposta mais eficaz e rápida.

Do ponto de vista legal, a repercussão dos cibercrimes também pode influenciar na criação e no aprimoramento das leis relacionadas à segurança cibernética. À medida que esses crimes se tornam mais sofisticados e generalizados, é fundamental que as legislações acompanhem.

CONCLUSÃO

A partir dos questionamentos levantados na introdução pode –se concluir que os crimes normais (ou crimes convencionais) e os cibercrimes diferem em vários aspectos devido à sua natureza e à maneira como são cometidos.

Sendo assim, os crimes convencionais ocorrem no mundo físico, envolvendo ações tangíveis, como roubo, agressão física, vandalismo, e também o perpetrador geralmente precisa estar fisicamente presente no local do crime assim deixando impressões digitais, DNA e testemunhas oculares.

Já os crimes cibernéticos ocorrem no mundo digital, utilizando computadores, redes e dispositivos eletrônicos para cometer atividades ilegais, como *phishing*, fraude online, os perpetradores podem estar em qualquer lugar do mundo, desde que tenham acesso à internet, então os rastros deixados são as evidências digitais, como registros de logs, endereços IP e registros de transações eletrônicas, são cruciais para rastrear os criminosos.

Em adendo, foi de notório interesse a inserção de informações gerais e básicas para compreendermos melhor o que são os crimes cibernéticos e como o Direito Penal legisla sobre esta modalidade de crime que cada veze se faz presente no nosso dia a dia.

Por conseguinte, pode ser destacado, ainda, que os desafios legais e técnicos associados à investigação e coleta de evidências em casos de crimes digitais são significativos e estão em constante evolução. Dessa forma, alguns dos principais desafios ao combate às faces dos crimes cibernéticos estão relacionados aos processos de anonimato e pseudônimos, Criptografia, Jurisdição cruzada, Exclusão ou alteração de evidências, Preservação de evidências, entre outros.

Outrora, não pode ser negado que, apesar de tais empecilhos, existem inúmeras instituições governamentais e não governamentais que agem para proteger a segurança digital e garantir a boa convivência no mundo virtual.

REFERÊNCIAS BIBLIOGRÁFICAS:

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, SEGURANÇA CIBERNETICA. Disponível em :<https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/>. Acesso em: 23 de novembro de 2023.

BARBOSA, Mateus Israel Alves Cruvinel. **Crimes virtuais a evolução dos crimes cibernéticos e os desafios no combate**, Artigo Científico (Graduação em Direito) – Escola de Direito e Relações Internacionais, Curso de Direito, Pontifícia Universidade Católica de Goiás, Goiânia/GO, 2020.

BRASIL. DECRETO N. 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: Presidência da República, 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm#:~:text=DECRETO%20N%C2%BA%2011.491%2C%20DE%2012,23%20de%20novembro%20de%202001>. Acesso em: 11 de marc 2024.

_____. **Lei Geral de Proteção de Dados Pessoais (LGPD)**, 13.709, de 14 de agosto de 2018.

COSTA, Luiz Fernando. **A TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS: Uma análise da adequação das leis existentes para lidar com os desafios e especificidades dos crimes cometidos no ambiente digital**, Artigo Científico (Graduação em Direito). Centro Universitário de Belo Horizonte, Belo Horizonte/MG, 2023.

CRIME INFORMÁTICO (Artigo). *In:* WIKIPEDIA, a enciclopédia livre. Flórida: Wikipedia Fundation, 2023. Disponível em: https://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico. Acesso em: 07 de nov 2023 às 10:57.

DUARTE, Karla Lorrany da Silva. **Crimes Cibernéticos Os Impactos da Lei Geral de Proteção de Dados**, Monografia (Graduação em Direito). UniEVANGÉLICA, Anápolis/GO, 2022.

EDITORIAL CÁTEDRA. **CRIMES CIBERNÉTICOS: DEFINIÇÃO E CONTEXTO**. *In:* Instituto e Desenvolvimento Profissional e Pós-Graduação (artigo *online*), 20 set 2019. Disponível em: <https://idcatedra.com.br/2019/09/crimes-ciberneticos-definicao-e-contexto/>. Acesso em: 07 de nov 2023.

FAQIM, Eduarda Queiroz *et al*. **Convenção de Budapeste sobre Crimes Cibernéticos**. *In:* Jusbrasil (artigo *online*), 2023. Disponível em: <https://www.jusbrasil.com.br/artigos/convencao-de-budapeste-sobre-crimes-ciberneticos/1665352986>. Acesso em: 09 de mar 2024.

FIA BUSINESS SCHOOL. ***Cyberbullyng:*** **O que é, consequências e dados no Brasil.** *In:* Fia Business School (artigo *online*), 06 jan 2023. Disponível em: < https://fia.com.br/blog/cyberbullying/>. Acesso em: 12 mar 2024.

FREITAS, V. V. M. S. de; SANTOS, W. B. dos; CURY, L. V. M. (2023). **CRIMES VIRTUAIS: UM OLHAR SOB A ÓTICA DO DIREITO PENAL.** *Revista Ibero-Americana De Humanidades, Ciências E Educação*, *9*(5), 1285–1304.

LORENZO, Larissa Papandreus; SCARAVELLI, Gabriela Piva. **Cibercrimes e a Legislação Brasileira.** Revista Científica do Curso de Direito, Centro Universitário FAG, Paraná, v. 4 n. 1 2021.

MALWAREBYTES. ***Phishing***. *In:* Malwarebytes (artigo *online*),2023. Disponível em: < https://br.malwarebytes.com/phishing/>. Acesso em: 25 mar 2024.

NEOWAY. **Fraudes na Internet: quais os tipos de golpes e como evitá-los**. *In:* Neoway (artigo *online*), 07 dez 2020. Disponível em: < https://blog.neoway.com.br/fraudes-na-internet/>. Acesso em: 25 mar 2024.

NETO, Mário Furlaneto; GUIMARÃES, José Augusto Chaves (2003). **Crimes na Internet : elementos para uma reflexão sobre a ética informacional**. *Revista CEJ*, *7*(20), 2003.

PEREIRA, Natália Ribeiro. **MARCO CIVIL DA INTERNET E A RESPONSABILIZAÇÃO DOS PROJETOS POSTADOS NA REDE: Uma comparação entre o Projeto de Lei 2126 de 2009 e a Lei 12.965 de 2014**, Projeto de trabalho acadêmico (Metodologia Científica do curso de Comunicação em Redes Sociais). Centro Universitário de Brasília (UniCEUB/ICPD), Brasília/DF, 2016.

PINHEIRO, Patrícia Peck. **Direito digital.** 2. ed. São Paulo: Saraiva, 2008.

ROSA, Fabrizio. **Crimes de Informática.** Campinas: Bookseller, 2002.

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal.** São Paulo: Memória Jurídica Editora, 2004.

SOUZA, Isabella Carrijo Campos Modesto. **A Evolução dos Crimes Cibernéticos e o acompanhamento das Leis Epecíficas no Brasil entre 2000 a 2020**. Monografia (Curso de Direito). Faculdade Evangélica de Rubiataba/GO, 2020.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático** / Spencer Toth Sydow -3. ed. rev. e atual. Salvador: Editora JusPodivm, 2022.

TORMEN, Chalidan Adonai Callegari. **Crimes Cibernéticos: (im)possibilidades de coerção**. Monografia (Graduação em Direito). Erechim/RS, 2018.

VANCIM, Adriano Roberto; NEVES, Fernando Frachone. **Marco Civil da Internet – Anotações à Lei nº 12.965/2014.** 2ª ed. Leme: Mundo Jurídico, 2015.