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

CRIMES CIBERNÉTICOS
E A LEGISLAÇÃO PENAL BRASILEIRA

ORIENTANDA: DEBORAH BATISTA NUNES
ORIENTADORA: PROFª. DRA. MARIA CRISTINA VIDOTTE BLANCO TARREGA

GOIÂNIA-GO
2023
DEBORAH BATISTA NUNES

CRIMES CIBERNÉTICOS
E A LEGISLAÇÃO PENAL BRASILEIRA

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).
Profª. Orientadora: Dra. Maria Cristina Vidotte Blanco Tárrega.

GOIÂNIA-GO
2023

DEBORAH BATISTA NUNES

CRIMES CIBERNÉTICOS
E A LEGISLAÇÃO PENAL BRASILEIRA

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientadora: Prof.ª. Dra. Maria Cristina Vidotte Blanco Tárrega. Nota

_____

Examinador (a) Convidado (a): Prof.ª Dra. Cláudia Luiz Lourenço Nota

SUMÁRIO

CRIMES CIBERNÉTICOS
E A LEGISLAÇÃO PENAL BRASILEIRA

Deborah Batista Nunes[1]

Tendo em vista que os crimes cibernéticos têm se tornado uma preocupação crescente no Brasil e em todo o mundo, este artigo científico tem como objetivo compreender de que forma eles vem ocorrendo e como puni-los. A legislação penal brasileira tem evoluído bastante para abordar esse desafio, criminalizando condutas relacionadas à atividade criminosa online. Através de leis como a Lei Carolina Dieckmann e o Marco Civil da Internet, o Brasil vem buscando punir e prevenir delitos como invasões de sistemas, fraudes eletrônicas, estelionato virtual, calúnia e difamação entre outros. Essas leis estabelecem penas e responsabilidades para indivíduos que praticam crimes cibernéticos.

Palavras-chave: Crimes cibernéticos. Legislação. Internet. Mundo virtual.

[1] Acadêmica em direito pela Pontifícia Universidade Católica de Goiás.

INTRODUÇÃO

O presente tema se dá devido a importância da tecnologia na atualidade, e que apesar de benéfica e facilitadora para a sociedade, essa evolução tecnológica também trouxe aspectos negativos no meio eletrônico pois com a facilidade dos aparelhos digitais juntamente com o uso das redes sociais, houve o crescimento dos crimes cometidos no âmbito virtual, é notório a relevância social haja vista o número de pessoas que vem sendo atingidas por tais criminosos, e a facilidade que estes tem de praticá-los. Seja no trabalho ou no lazer, basta olhar para o outro lado e perceber a presença de aparelhos eletrônicos que passam a maior parte do tempo se comunicando e interagindo. Por outro lado, temos que estar atentos ao fato de que os criminosos estão com as armas do crime nas mãos, nos bolsos, e ninguém percebe o ato, ou quando vem perceber já causou algum prejuízo.

A metodologia a ser utilizada na elaboração da pesquisa envolverá o método dedutivo e a pesquisa teórica, utilizando a legislação, pesquisas bibliográficas, doutrinas e artigos. A pesquisa fará uso de métodos científicos para uma boa compreensão do tema desenvolvendo dentro dos limites dos objetivos propostos. A referência bibliográfica será de grande importância, pois nos fornece um estudo teórico, embasado na lei, na doutrina e artigos científicos. Serão realizados vários procedimentos metodológicos, a partir da pesquisa bibliográfica.

Com o estudo desenvolvido nesse trabalho conheceremos os crimes cometidos pelos meios eletrônicos, quem é o autor, a vítima, a forma de cometê-los, a legislação que se aplica a eles. A fundamentação teórica do presente artigo apresentará o conhecimento sobre crimes cibernéticos, e toda sua evolução histórica. Serão apresentados conceitos, espécies, contexto histórico, formas de praticá-lo, e a legislação vigente acerca do assunto.

O objetivo geral será entender o conceito de crimes cibernéticos, analisar as leis vigentes e compreender de que forma são cometidos no âmbito virtual.

1 EVOLUÇÃO HISTÓRICA DOS CRIMES CIBERNÉTICOS

A internet pode ser considerada atualmente uma grande evolução social que trouxe a revolução tecnológica, onde traz a comunicação facilitada em qualquer lugar do mundo, no entanto, com essa evolução rápida, o mundo virtual despertou em criminosos, novas oportunidades de aproveitamento, a serem tomados por práticas de crimes, havendo uma migração desses bandidos com objetivo de apoderar-se dessas informações para obter vantagem iniciando uma nova categoria de crimes sendo denominados como cibernéticos

Os crimes cibernéticos se deram com a cibercriminalidade, que é uma ferramenta utilizada por muitas pessoas hoje em dia, no entanto a idealização de hoje, não é a mesma do início de sua história.

Anteriormente valorizava-se o trabalho braçal, principalmente as pessoas que não tinham uma condição social elevada, no momento em que as novas tecnologias chegavam ao mundo a população repudiava a ideia, de utilizar uma máquina, no primeiro momento se tratava de desconhecimento e no outro receio que fossem substituídos por inovações tecnológicas.

Jesus expõe sobre o assunto:

> Trago como exemplo a sabotagem dos funcionários de Joseph-Marie Jacquard, inventor do tear mecânico, pois, em suas concepções, colocava seus empregos em risco. É claro que o conceito de crimes informáticos somente ganhou contornos mais específicos algumas décadas depois. Jesus e Milagre explica que a doutrina ainda diverge sobre qual seria o primeiro crime informático propriamente dito da história, dividindo-se entre dois acontecimentos de duas universidades norte americanas, uma em 1964 e outra em 1978, em que estudantes invadiram o sistema de dados computadorizados das instituições. (Jesus, 2016, p.22).

Desta forma, se deram dois acontecimentos que marcaram de forma incisiva para início dos crimes cibernéticos, sendo os primeiros casos ocorridos dentro de duas Universidades Americanas, em 1964 e outro 1978 que invadiram o sistema de dados computadorizados das instituições.

Insta ressaltar que a computação teve seu avanço em 1946, nos Estados Unidos, com surgimento do primeiro computador totalmente eletrônico, uma máquina que pesava 30 toneladas e milhares de componentes.

Com essa nova evolução, a informática se tornou algo cotidiano das pessoas que viviam na época da Revolução Industrial, conforme afirma Medeiros:

> Os modernos sistemas computacionais e o aprimoramento das aplicações tecnológicas em vigor vão sendo lançados no mercado sempre na ânsia de melhorar e facilitar a forma de nos comunicarmos, permitindo, inclusive, que os diversos países, como no caso o Brasil, pudesse ser integrados ao mundo globalizado sob diversos aspectos. (Medeiros, 2010, p.2).

Os primórdios dessa evolução se deram com a criptografia que era conhecida como uma linguagem codificada, que era utilizada no período da Grécia e a Pérsia emergiram-se a necessidade de transmitir as informações secretamente, para que somente o destinatário final pudesse entender o que estava descrito.

A partir daí a criptografia emergiu-se em parâmetros imensos ao longo dos séculos, pois naquela época existiam muitos segredos de guerra e do governo, este não poderia ser decifrado por qualquer pessoa, por isso para ocultar essas informações tratava-se de forma quase científica, tendo as primeiras noções muito rudimentares da cibercriminalidade, advindos de informações sigilosas que era necessário um perito com técnicas adequadas para decifrar os códigos.

A ideia da construção de uma rede de computadores que pudessem trocar informações surgiu neste projeto, idealizado por Licklider, uma rede de computadores que permitisse o trabalho coletivo em grupos, mesmo que fossem interligados por pessoas geograficamente distantes, além de permitir o compartilhamento de recursos escassos, como por exemplo, o supercomputador ILLIAC IV, que na época estava em construção na Universidade de IIlinois.

Para realizar o primeiro experimento com a rede foram escolhidas quatro Universidades que seriam conectadas em janeiro de 1970 na rede, a rede incluía computadores de várias plataformas sendo “hardware e de software. Com passar dos anos, o computador se interlaçou com o mundo, caracterizado no ambiente virtual conhecido como ciberespaço, iniciou-se todo tipo de relação, tratando-se de ambiente alheio a realidade física que vem influenciando nas ações humanas e surgindo novos tipos delitos.

1.1 CONCEITO DE CRIMES CIBERNÉTICOS

São também chamados de crimes virtuais, cibercrimes, crimes da internet, e consistem em atividades ilícitas praticadas por um ou mais criminosos por meio de dispositivos eletrônicos e da internet.

Os crimes cibernéticos consistem no cometimento de atividades ilícitas por meio do computador ou rede de internet e classificam-se de acordo com a sua forma de cometimento. (Wendt; Jorge, 2012).

Segundo o doutrinador Jesus *apud* Carneiro (2012, n.p.):

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. Crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço “real”, ameaçando ou lesando outros bens, não computacionais ou diversos da informática.

Estes são caracterizados, como pirataria, pornografia infantil, calúnia, difamação, injúria, estelionato, dentre outros, sendo crimes graves, como por exemplo, a pornografia infantil incluída como crime no artigo 241 do Estatuto da Criança e do Adolescente:

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008).

Já com relação á injúria e calúnia este são caracterizadas como crimes contra a honra e estão regulamentados nos artigos 138, 139 e 140 do Código Penal.

Desta forma podemos observar que todos estes crimes são caracterizados de forma física e digital, determinando um parâmetro da modificação nos textos legais, buscando até adaptação para que determinados delitos sejam reconhecidos como crimes pelo mundo.

Mesmo havendo diversas mudanças legislativas, ainda a informatização carece de uma legislação mais ativa, de modo que os aplicadores da lei sejam obrigados a enquadrar as condutas de acordo com tipos penais referentes ao crime cometido, buscando enrijecer o sistema jurídico brasileiro.

1.2 NOÇÕES SOBRE CIBERCRIMINALIDADE

A cibercriminalidade foi determinada pela primeira vez em uma reunião no Grupo de países na época considerados os mais desenvolvidos, conhecidos como grupo G-8, nessa discussão falavam sobre a necessidade do combate às práticas ilícitas que ocorriam na internet.

Conforme determina Sismas sobre o conceito de cibercriminalidade:

> O cibercriminalidade nada mais é que todo ato em que o computador ou meios de tecnologia da informação serve para atingir um ato criminoso ou em que o computador ou meios de tecnologia da informação é objeto de um crime. O cibercrime está relacionado ao fenômeno da criminalidade informacional de condutas violadoras de direitos fundamentais, seja por meio da utilização da informática para praticado crime como elemento do tipo penal. (Sismas, 2014, p.14).

A cibercriminalidade é toda atividade criminosa realizada por computadores ou meios de tecnologia da informação, sendo este meio uma parte do tipo penal, mesmo que bem jurídico esteja protegido.

Geralmente é realizada por Hackers, este termo e importado da língua inglesa são utilizados para designar programadores, que buscam por meio do sistema de informações de pessoas, empresas, órgãos governamentais e tudo que está disposto na rede.

O Hacker é conceituado por Pantulho (2010, p. 1) como:

> É uma pessoa física que detém, como objeto, a investigação da integridade e da segurança de um sistema qualquer de computador. Utilizasse de técnicas avançadas para invadir sistema e detectar suas respectivas falhas todavia não destrói ou prejudica.

Com isso, devemos entender que os indivíduos que são hackers, possuem um grande conhecimento de programação e de segurança dos sistemas de computação, podendo-se utilizar para tirar vantagens pessoais, cometendo inúmeras condutas criminosas determinando para diversos fins ilícitos no sistema eletrônico.

Nos dias atuais, há diversas facilidades nas compras online acesso a conta bancário diante de um simples celular ou através de tela de computador, geralmente sem preocupação se site em que estamos realizando está compra é seguro, nos tornando alvo fácil para quem está acostumado a praticar o cibercrime.

Insta salientar que na maioria das vezes os autores dessas práticas delituosas são dotados de conhecimentos específicos e já foram batizados pela comunidade cibernética como os agentes delituosos no cometimento destes crimes.

Cada um desses indivíduos que são com esses sistemas é classificado de forma diferente, como por exemplo, o conhecido como “Cracker” ele não comete condutas delituosas, ao contrário, criam novos programas e utilizam suas habilidades na consecução de sistemas., este e considerado um expert na quebra de um sistema de segurança, sendo um codificador de programas.

Temos também os especialistas no estelionato determinado como “Carder”, estes tiram proveitos de algumas falhas na segurança de bancos, de cooperativas de crédito e sites, se passando por vendedores para retirada de informações importantes, para utilizarem de forma criminosa.

Outro indivíduo que trabalha com a cibercriminalidade é o Phreaker, esse busca rastrear dados via telefônica, para modificá-los internamente essas linhas para manter o contato diretamente para ter os domínios das linhas para fazer ligações gratuitas e clandestinas.

Segundo Crespo (2011, p. 1) determina o conceito de Phreaker:

> Fazem com que as operadoras se confundam quanto á origem de uma ligação permitindo, assim, que o usuário legítimo que utiliza os serviços de determinada telefonia pague pela ligação realizada pelo delinquente.

Outra subdivisão trata do Defacer estes deixam marcas em sites, através de mensagens de protesto contra uma causa ou contra o próprio site, já Spammer este espalha e-mails com correntes e vírus que danificam ou roubam informações de usuários, desde dados pessoais á dados bancários.

E por último Cyberpunk que causam danos as vítimas por prazer, podendo ser pela queda do servidor ou até mesmo pela eliminação completa dos dados armazenados, podendo aplicar golpes aos usuários.

Importante salientar que a atuação destes agentes delituosos é cometida no anonimato e por isto, a polícia encontra muitas vezes dificuldade na identificação. Em outros casos, estes agentes utilizam pseudônimos, dados falsos para praticar os delitos.

A fraude acontece, nos dias atuais por meio de uso de ferramentas virtuais, podendo se passar por uma mensagem não identificada, por uma comunicação falsa

de uma instituição verdadeira conhecida, como um banco procurando induzir o destinatário vítima a compartilhar informações como senhas e dados pessoais financeiros.

Outro ponto importante de salientarmos é sobre o surgimento da “dark web” é termo utilizado para classificar partes da internet que estão escondidas e podem ser de difícil sem a utilização de um software especial. Essas paginam também não podem ser encontradas por meio de uma pesquisa em sites de busca como o Google.

Desta forma, podemos constatar que os crimes derivados dos cibercrimes, vem tomando uma realidade desproporcional, alcançando cada vez mais o mundo real, surgindo a necessidade de uma legislação mais rígida, sendo culpável de acordo com sua complexidade, apesar de haver algumas legislações cada vez torna-se difícil de aplicar a penalização devido o anonimato.

2 ESPÉCIES DE CRIMES CIBERNÉTICOS

A internet possibilita um mundo utópico no qual as pessoas encurtam as distâncias físicas, conectando-se a outras e se encorajam através do anonimato. (Pannain e Pazzella, 2015, p.28).

Grande parte dos crimes que ocorrem no meio virtual também ocorrem na vida real, nota-se que esse ambiente trás uma sensação de segurança e anonimato tornando ainda mais propício para a prática de tais crimes.

A seguir serão abordadas algumas das principais espécies dos crimes que vem ocorrendo através do mundo virtual.

2.1 CRIMES CONTRA A HONRA DIANTE DAS REDES SOCIAIS

Com a amplificação do acesso ao ambiente virtual a um grande número de pessoas, nota-se que houve um crescimento da prática dos crimes contra a honra também nesse mundo da internet, previstos no Código Penal de 1940, estas condutas prejudicam a integridade moral e ferem a dignidade e honra das vítimas (Capez, 2022, p.3).

Existem três tipos de crimes contra a honra, sendo: calúnia, difamação e injúria. Tais crimes quando ocorridos perante as redes sociais podem ter a pena aumentada como prevê o artigo 141, §2º do código penal: “se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena”.

A honra é um bem jurídico protegida constitucionalmente, sendo um direito fundamental (art. 5º, X, Constituição Federal). Todavia está ligada a dignidade da pessoa humana, já que diz respeito a sua reputação (Barroso, 2004, p. 4). Pode ser subdividida em honra objetiva e subjetiva, na objetiva tem como característica a imagem que a pessoa carrega diante da sociedade em que convive, ou seja, como somos vistos pelos outros. Já se referindo a honra subjetiva é o sentimento pessoal relacionado as qualidades físicas intelectuais e sociais, qualidades que a pessoa procura ter. (Rodrigues, 2016).

O Código Penal em seu artigo 138 tipifica calúnia: “caluniar alguém, imputando-lhe falsamente fato definido como crime”. A difamação está prevista no ordenamento jurídico, no artigo 139 do Código Penal, como “difamar alguém, imputando-lhe fato ofensivo à sua reputação”. Por fim, a injúria é definida no artigo 140, como “injuriar alguém, ofendendo-lhe a dignidade ou o decoro”.

Em relação ao tema, veja-se análise do doutrinador Cunha (2014, p. 86):

> Na calúnia e na difamação tem-se a presença de uma conduta específica de imputar a alguém um fato concreto e ofensivo, necessariamente falso e definido como crime no caso da calúnia – requisitos não exigidos na difamação. A injúria, por sua vez, trata-se de uma imputação genérica, uma má qualidade, um defeito ou algo que menospreze a vítima. Nas duas primeiras, exige-se que a frase desonrosa chegue ao conhecimento de terceiro, o que é desnecessário para a última.

Ainda sobre os crimes mencionados acima Silva, Bezerra e Santos (2016, p. 132) pontuam:

> As múltiplas possibilidades do uso dos computadores e das ferramentas online levaram o Estado a constatar que não estava necessariamente preparado para julgar e punir usuários potencialmente criminosos, cujas ações atingem a honra, o decoro e a dignidade de terceiros.

Em regra, os crimes contra a honra precisam de ser denunciados pela vítima em uma delegacia, e como a lei comina pena máxima de 2 anos para esses crimes, as ações tramitarão perante os juizados especiais criminais.

Sobre a investigação dos crimes no meio virtual Junior destaca:

> Para que ser apurado um crime digital é necessária à coleta de dados em provedores de acesso. Considerando que os provedores de serviços, de conteúdos e as redes sociais como o Facebook, dentre outros, somente apresentam esses dados por meio de ordem judicial, se fazendo necessário processar tais provedores para que os dados de conexão relativos ao usuário de seus serviços que tenha praticado algum crime virtual ou causado danos a alguém sejam apontados. (Junior, 2015, p. 30)

Com isso nota-se a complexidade de apurar os crimes cibernéticos, vez que é muito fácil para o criminoso tentar apagar os vestígios como por exemplo de mensagens ofensivas a alguém.

2.2 ESTELIONATO VIRTUAL

O estelionato está previsto no artigo 171, do Código Penal, e pode ser praticado tanto no âmbito virtual, como fora dele. Com o grande avanço da tecnologia a prática desse crime tem aumentado drasticamente, com o intuito de combater esse crime entrou em vigor a lei nº 14.155/21 que trouxe para o ordenamento jurídico a modalidade qualificada dos crimes de furto e estelionato praticados por meio da internet.

No âmbito virtual o estelionato ocorre quando o agente pratica uma conduta de “induzir ou manter a vítima em erro, e com isso, obtém vantagem ilícita, para si ou para outrem”. O principal objetivo é induzir a vítima a erro para que ela forneça de forma espontânea seus dados pessoais, bancários o que possibilitará o agente formas mais fáceis de obter vantagens no nome da vítima.

Sobre o assunto leciona Guilherme Feitoza:

> Uma das formas mais recorrentes do estelionato no ciberespaço é a invasão do correio eletrônico da vítima, em particular o daquelas pessoas que possuem o costume de consultar seus saldos e extratos bancários pelo computador. Nesta situação, o estelionatário (*crackler*) encontra alguma maneira de clonar a página legítima do internet banking do usuário e fazer com que ele tente fazer o acesso, sem saber que os dados que estão sendo inseridos serão interceptados por um terceiro de má-fé que irá usá-los indevidamente. (Feitoza, 2012, p.48)

Nos dias atuais está cada vez mais comum a prática de golpes por meio da internet como por exemplo golpes e fraudes associados ao pix, um dos mais comuns se trata do “pix multiplicador”, os golpistas enviam através das redes sociais uma suposta tabela com um valor inicial que eles chamam de investimento, prometendo um valor muito mais alto que a vítima receberia em poucos segundos após realizar a

transferência, ocorre que feito a transferência do suposto investimento a vítima não recebe nenhum valor como havia sido prometido, perdendo então o seu dinheiro e se consumando o golpe.

2.3 DA INVASÃO DE DISPOSITIVO ELETRÔNICO

Previsto no artigo 154 – A do Código Penal esse crime consiste na Invasão de dispositivo informático de uso alheio, o crime é consumado quando um criminoso invade um dispositivo mediante violação dos mecanismos de segurança com a finalidade de adulterar, obter ou destruir dados ou informações sem autorização do usuário.

Nucci dispõe sobre o assunto:

> A nova figura típica de invasão de dispositivos informáticos, insere-se no contexto de crimes contra a liberdade individual, sendo este o bem jurídico mediato tutelado. No entanto, de forma imediata, ingressou-se no campo dos crimes contra a inviolabilidade dos segredos, com proteção acerca da intimidade, da vida privada, da honra, da inviolabilidade de comunicação e correspondência, enfim, da livre manifestação do pensamento, sem nenhuma intromissão de um terceiro. (Nucci, 2014)

Nota-se então que o bem jurídico protegido pelo ordenamento são os interesses pessoais que estão armazenados no dispositivo da vítima, e não o dispositivo informático em si. Em relação a ação penal desse crime o artigo 154 – B do Código Penal prevê que a ação deve proceder mediante ação penal pública condicionada a representação, sendo necessária a autorização da vítima para propor a ação penal. Porém se for 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, a legislação prevê a ação penal incondicionada.

3 A LEGISLAÇÃO VIGENTE DIANTE OS CRIMES CIBERNÉTICOS

Considerando a popularidade da internet dos dias atuais, é notório que a legislação ainda está em processo de formação. Dessa forma, até um passado

recente os crimes praticados no ambiente virtual eram tipificados analogicamente em tipos penais comuns (Tavares, 2012).

Ainda há desafios da legislação diante a dificuldade de investigação dos sujeitos ativos dos crimes, pois a tecnologia facilita a ocultação da autoria, e, portanto, para identificar o criminoso teria que obter o IP, login e senha do dispositivo utilizado para praticar o crime, porém estes podem utilizar informações falsas, o que dificulta o trabalho investigativo (Siqueira 2017, p. 122).

3.1 LEI Nº 12.737/2012 “CAROLINA DIECKMANN”

Essa lei ficou popularmente conhecida como lei Carolina Dieckmann em razão do episódio com a atriz, que em maio de 2012, teve seu computador invadido por criminosos onde foi divulgado várias fotos íntimas, causando um grande transtorno e constrangimento à vítima. Ressalta-se que a referida lei transitava na câmara desde 1999, mas só foi sancionada após a comoção do caso da atriz Carolina Dieckmann, introduzindo então no Código Penal brasileiro o tipo nominado “Invasão de dispositivo informático” já estudado na sessão anterior.

Sobre isso dispõe Masson:

> Como de praxe, os debates sobre uma legislação específica para os crimes ligados à internet (crimes cibernéticos) se arrastavam há anos, em velocidade de conexão discada. Mas a atividade dos congressistas, impulsionada pela opinião pública, recebeu imenso upload depois da invasão do computador pessoal de Carolina Dieckmann. (Masson, 2017)

Inicialmente foi previsto pena de detenção de três meses a um ano para esses crimes, entretanto recentemente foi aprovado a lei 14.155/21 que aumentou a pena para um a quatro anos de reclusão.

Ocorre que somente a lei 12.737 não foi suficiente, o que restou a elaboração de novas legislações acerca do assunto como a lei 12.965 conhecida como marco civil da internet, ela foi criada para estabelecer princípios, garantias, direitos e deveres para o uso da internet, bem como determinou as diretrizes para a atuação da União, Estados e Municípios.

Sobre a intenção do marco civil da internet Siqueira leciona:

> A lei do Marco Civil foi criada para suprir as lacunas no sistema jurídico em relação aos crimes virtuais, num primeiro momento tratando dos

> fundamentos, conceitos para sua interpretação e objetivos que o norteiam, além de enumerar os direitos dos usuários, tratar de assunto polêmicos como por exemplo a solicitação de histórico de registros, a atuação do poder público perante os crimes virtuais e por último garante o exercício do direito do cidadão de usufruir da internet de modo individual e coletivo estando devidamente protegido. (Siqueira 2017, p. 126).

Contudo, a referida lei tem como objetivo fornecer uma segurança jurídica para os usuários da rede. Pode ser que ainda não seja o suficiente para o combate de tais crimes, no entanto é um avanço considerável.

3.2 A LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), foi sancionada em 2018, mas entrou em vigor somente no ano de 2020. Ela veio com o objetivo de estabelecer uma segurança jurídica e proteger os dados pessoais de todos os cidadãos presentes no território brasileiro, ela define esses dados como todas as informações que possam identificar um indivíduo como o Rg, CPF, número de telefone, endereço residencial, contas bancárias, renda, histórico de pagamentos, retrato em fotografia, entre outros. (Serpro, 2020, *online*).

Somadossi expõe sobre o assunto:

> Dentre seus princípios, tem especial relevância o da transparência para o uso de dados pessoais e a respectiva responsabilização, o da adequação, ou seja, a compatibilização do uso dos dados pessoais com as finalidades informadas, da proteção do usuário em toda arquitetura do negócio *(privacy by design)*, da finalidade, segundo o qual os dados só devem ser utilizados para as finalidades específicas para as quais foram coletados e previamente informados aos seus titulares, e também do princípio da necessidade, que significa limitar o uso dos dados ao mínimo necessário para que se possa atingir a finalidade pretendida, do qual surge ainda a indispensável exclusão imediata de dados, após atingida tal finalidade. (Somadossi ,2018, *online*)

Outro ponto importante abordado pela lei é a questão do consentimento, que deve ocorrer de forma livre, onde o titular expresse autorização com o tratamento de seus dados para uma finalidade específica, não admitindo autorizações genéricas, ocorrendo a vedação do tratamento caso a autorização tenha ocorrido mediante vício de consentimento. (Serpro, 2020, *online).*

A fiscalização acerca do cumprimento da LGPD é feita pela Autoridade Nacional de Proteção de Dados Pessoais, a ANPD, onde são necessários também

agentes de tratamento de dados, os quais tem suas funções estipuladas pela própria Lei de Proteção de Dados (Brasil, 2020, *online*).

Com relação as falhas de segurança que vier ocorrer, estas podem gerar multas de até 2% do faturamento anual da organização no Brasil, e no limite de 50 milhões por infração. (Serpro, 2020, *online*).

CONCLUSÃO

Ao fim da pesquisa pode-se concluir que o assunto é de alta relevância na atualidade, pois se trata de uma prática que vem aumentando de forma drástica, sendo uma consequência do avanço tecnológico, da expansão e da popularidade da internet.

Em conclusão, o artigo abordou a evolução dos crimes cibernéticos em paralelo com o avanço da tecnologia e da internet. A revolução tecnológica proporcionou uma comunicação facilitada em todo o mundo, mas também deu origem a essa nova categoria de crimes: os crimes cibernéticos dos quais variam desde a invasão de dispositivos eletrônicos até crimes contra a honra, estelionato virtual entre outros.

Contudo, a legislação brasileira tem avançado para combater esses crimes, com leis como a "Lei Carolina Dieckmann" e o "Marco Civil da Internet", que estabelecem princípios e diretrizes para o uso da internet e tratam de questões relacionadas à invasão de dispositivos informáticos e à proteção de dados pessoais. Além disso, a Lei Geral de Proteção de Dados (LGPD) estabelece regras para o tratamento de dados pessoais e a responsabilização das organizações que não cumprirem essas regras.

Portanto, mesmo com a evolução da legislação sobre o assunto ainda há muitos desafios no combate aos crimes cibernéticos, como a dificuldade de identificação dos criminosos devido ao anonimato que a internet proporciona sendo fundamental que a legislação continue a evoluir e que sejam desenvolvidas

estratégias eficazes para lidar com esse tipo de criminalidade que está em constante evolução.

Por fim, a internet trouxe inúmeras vantagens para a sociedade, mas também abriu portas para novos tipos de crimes. A resposta a esses desafios deve envolver aprimoramentos na legislação para que haja punição severa a esses criminosos, maior conscientização e medidas de segurança cibernéticas para proteger os indivíduos e as organizações contra ameaças virtuais.

ABSTRACT

Considering that cybercrimes have become a growing concern in Brazil and around the world, this scientific article aims to understand how they are occurring and how to punish them. Brazilian criminal legislation has evolved significantly to address this challenge, criminalizing conduct related to online criminal activity. Through laws such as the Carolina Dieckmann Law and the Marco Civil da Internet, Brazil has sought to punish and prevent crimes such as system invasions, electronic fraud, virtual fraud, slander and defamation, among others. These laws establish penalties and responsibilities for individuals who commit cybercrimes.

Keywords: cybercrimes. Legislation. Internet, virtual world.

REFERÊNCIAS

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A Trajetória Da Internet No Brasil: Do surgimento das redes de computadores à instituição dos mecanismos de governança**. Publicado pela UFRJ, 2006.

CASTILHO, Ricardo. **Direitos Humanos.** 6. Ed. São Paulo: Saraiva Educação, 2018.

CAPEZ, S. P. F. **Codigo Penal Comentado.** 3. ed. São Paulo: saraiva, 2012.

CUNHA, Rogério Sanches. **Manual de Direito Penal: Parte Geral**. Salvador: Juspodivm, 2014.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011.

FEITOZA, Luis Guilherme de Matos. **Crimes Cibernéticos: O estelionato virtual.** Brasília 2012.

GOV.BR. **Serpro e LGPD: segurança e inovação**. Gov.br. Disponível em: https://www.serpro.gov.br/lgpd. Acesso em: 13 set 2023.

JESUS, Damásio E.de. **Direito Penal**. 27. ed.v.1. São Paulo: Saraiva, 2003.

JESUS, Damásio de, e MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

MASSON, Cleber. **Código Penal comentado. 5ª ed**. São Paulo: Método, 2017.

MEDEIROS, Claudia Lucio de. **Deficiências da legislação penal brasileira frente aos crimes cibernéticos**. 2010.

NUCCI, Guilherme de Souza. **Código Penal Comentado. 14ª** ed. Rio de Janeiro: Forense, 2014.

PLANTULLO, V. L. **Estelionato Eletrônico**. Crutiba: Juruá, 2002.

PANNAIN, Camila Nunes; PEZZELLA, Maria Cristina. **Liberdade de Expressão e Hate Speech na Sociedade da Informação**. Revista Direitos Emergentes da Sociedade Global, Santa Maria, 2015.

RODRIGUES Júnior, Celso. **A caracterização do crime de difamação por meio de postagem em rede social.** 2016.

SANTIAGO, Emerson. **Liberdade de Expressão**. Ano 2015.

SISNEMA, **Informática. Cracker e Hacker**. 2012. São Paulo.

SOMADOSSI, Henrique. **O que muda com a Lei Geral de Proteção de Dados** (LGPD). Migalhas nº 4.478 24 de agosto de 2018. Disponível em:

https://www.migalhas.com.br/depeso/286235/o-que-muda-com-a-lei-geral-de protecao-de-dados--lgpd. Acesso em 13 set 2023.

TAVARES, José de Farias. **Comentários ao Estatuto da Criança e do Adolescente**. Rio de Janeiro: Forense, 2012.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos: Ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p 10.