PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNCAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

CIBERCRIMES E OS REFLEXOS NO DIREITO BRASILEIRO

ORIENTANDA - MYKAELLY SOUZA

ORIENTADORA – PROF. GOIACYMAR CAMPOS DOS SANTOS

GOIÂNIA
2021

MYKAELLY SILVA SOUZA

CIBERCRIMES E OS REFLEXOS NO DIREITO BRASILEIRO

Monografia Jurídica apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
PROF. GOIACYMAR CAMPOS DOS SANTOS

GOIÂNIA/GO
2021/2

MYKAELLY SILVA SOUZA

CIBERCRIMES E OS REFLEXOS NO DIREITO BRASILEIRO

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador (a): Prof. Goiacymar Campos dos Santos
Nota

_____

Examinador (a) Convidado (a): Prof.: Prof. Fernando Gomes Nota

RESUMO

Conforme a tecnologia vai se aprimorando e a internet vai se expandindo, se tornando cada vez mais popular, os indivíduos passam a correr um risco maior de ser tornarem vítimas do cibercrime, sendo, portanto, necessário uma legislação eficaz para o combate e prevenção dessas condutas. O presente trabalho faz uma análise sobre a criação da internet e demonstra o que é o cibercrime e o cibercriminoso, bem como, analisa a tipicidade das principais condutas ilícitas praticadas no ambiente virtual. Tem como objetivo analisar os principais marcos na legislação brasileira referente aos crimes virtuais, abordando desde as primeiras medidas até as legislações atuais. A presente monografia foi moldada por meio de análises de posicionamentos doutrinários, antigas e vigentes legislações, utilizando-se de referências bibliográficas e uma abordagem dedutiva. Após a elaboração de três capítulos, foi concluído que o cibercrime ainda é um desafio para o direito brasileiro, não tendo as legislações conseguido acompanhar a intensa e rápida evolução da tecnologia e dos crimes virtuais.

Palavras chaves: Internet. Crimes Virtuais. Cibercriminoso. Legislação aplicável.

Sumário

INTRODUÇÃO

O avanço da tecnologia possibilitou uma alta circulação de informações, pessoas e mercadorias. Por meio desse avanço, surgiu a internet, que ensejou que o número de pessoas com acesso aos meios digitais (celulares, computadores, tablets, etc) crescesse em grande proporção. Assim, com o advento da internet, surgiram também novos meios de interação social, facilitando a coleta e compartilhamento de dados pessoais, além da comunicação com diferentes pessoas em qualquer lugar do mundo.

A internet se tornou um instrumento de comunicação e transmissão de informações, bem como de interação entre pessoas para as mais diversas atividades, nos mais diversos lugares do mundo. No entanto, a população passou a conviver não só com os benefícios advindos dessa inovação, mas também com seus malefícios. Diante da facilidade e rapidez com que as informações são compartilhadas e as interações são feitas, indivíduos passaram a utilizar a internet para praticar condutas ilícitas, conhecidas como crimes cibernéticos.

No ambiente virtual são praticados os mais diversos crimes cibernéticos. Informações, dados pessoais, contas bancárias, fotos, vídeos e conversas intimas são violadas, o que fere a dignidade humana, trazendo prejuízos imensuráveis às vítimas. Diante do surgimento dessas práticas ilícitas, tornou-se necessário a intervenção do Direito Penal, a fim de garantir a aplicação de normas penais na esfera digital. O Estado brasileiro, criou algumas leis e adotou algumas medidas, para tentar combater, de forma eficaz, esses tipos de delitos, o que vem sendo aprimorado, principalmente diante da pandemia do novo Coronavírus, em que foi necessário o isolamento social, aumentando ainda mais o uso da internet e das redes sociais.

É notório que o tema abordado se trata de uma questão da atualidade, que precisa ser estudada e aprofundada, uma vez, que os crimes virtuais fazem milhares de vítimas todos os dias e são praticados das mais diversas formas. Ademais, a Constituição Federal assegura a inviolabilidade, intimidade, honra e vida privada, o que é o afetado por esses tipos de infrações. Assim, é necessário analisar de que forma o Direito Brasileiro se adaptou a essa nova realidade tecnológica e o que ainda pode ser feito para garantir a aplicação de normas penais de forma mais eficaz.

O presente trabalho tem como objetivo apresentar e explicar o que são e quais são os principais crimes praticados nos ambientes virtuais no Brasil e analisar quem são os cibercriminosos. Ademais, analisa e demonstra os reflexos dessas condutas criminosas no direito brasileiro.

Foi realizado com base em livros, artigos científicos, documentos e estudos do caso. É teórico, explicativo e descritivo, contando com uma investigação, registro, análise e interpretação de fenômenos atuais, objetivando o seu funcionamento no presente, com o intuito de aprofundar mais sobre o tema abordado, discorrendo os pontos mais criteriosos e importantes.

O primeiro capítulo abordará aspectos históricos e conceituais sobre a internet e cibercriminalidade, estudando sobre o surgimento e evolução dos mesmos, além de analisar quem são os cibercriminosos.

O segundo capítulo estudará os tipos penais dos crimes cibernéticos, demonstrando e explicando quais são os crimes virtuais mais cometidos no Brasil.

O terceiro capítulo abordará sobre a legislação brasileira aplicável sobre o cibercrime, desde as primeiras medidas até a legislação atual.

Dessa forma, o objetivo principal do presente trabalho é demonstrar o que é o cibercrime e os reflexos desses delitos Direito Brasileiro, desde os primeiros projetos de lei até a legislação atual.

1. ASPECTOS HISTORICOS E CONCEITUIAS DA INTERNET E DA CIBERCRIMINALIDADE

É notório que ao longo da história o ser humano buscou aprimorar as formas de comunicação e informação, a fim de unir diferentes povos, independentemente da distância, religião ou etnia. Por meio de um processo de evolução, através de muitos estudos, pesquisas e inventos, foi possível chegar a era da tecnologia.

Grandes avanços tecnológicos foram alcançados durante o século XX, momento em que houve o surgimento de meios digitais, tais como os computadores, que contribuíram na criação da internet, no ano de 1969.

A internet revolucionou o comportamento humano e se tornou indispensável na vida dos indivíduos, resultando em uma geração dependente da informática.

É crescente o número de pessoas com acesso aos meios digitais, que estão sendo, cada vez mais, aperfeiçoados, facilitando a comunicação e a transmissão de informações em qualquer lugar do mundo, e substituindo muitos atos da vida comum pelos sistemas informatizados.

Essa nova realidade social trouxe grandes progressos e facilidades, no entanto, também se tornou um meio para a realização de condutas ilícitas perigosas, tornando as pessoas vulneráveis à riscos inerentes a tecnologia da informação. Tais condutas são conhecidas como crimes virtuais e existem nas mais diversas formas.

1.1 NOÇÕES GERAIS SOBRE A INTERNET

A internet é uma extensa rede de computadores interligadas no mundo inteiro e plugadas por meio de cabos, linhas discadas (telefônicas), tecnologia de micro-ondas, satélite de comunicações e outros meios de telecomunicações.

> A internet é um conjunto de redes de comunicações em escala mundial e dispõe de milhões de computadores interligados pelo protocolo de comunicação TCP/IP, que permite o acesso a informações e todo tipo de transferência de dados. A Internet carrega uma ampla variedade de recursos e serviços num espaço virtual também chamado de ciberespaço, daí que,

> como no mundo real, a segurança digital é um terreno de ferrenha disputa entre defensores e agressores. (CASSANTi, 2014, p. 01)

Foi desenvolvida na época da guerra fria, através de projetos conduzidos ao longo dos anos 60 pela DARPA (Defense Advanced Research Projects Agency) que criou uma rede experimental de computadores, a ARPANET.

O seu desenvolvimento teve caráter militar, como um modo alternativo de comunicação entre os principais centros militares de comando e controle, caso os meios de comunicação utilizados na época fossem destruídos, ou seja, os militares, tinham por objetivo manter informações interligadas eletronicamente por computadores, de modo que não houvesse um comando central, pois, assim, em caso de ataque a um dos pontos da rede, a conexão ainda ficaria ativa (MORAES, 2004).

A ARPANET é de origem norte-americana, mas se expandiu e permitiu a conexão de outros websites em diversas universidades e centros tecnológicos do mundo, entre os anos de 1970 e 1980, estendendo o seu uso para uma motivação mais cultural e acadêmica do que militar.

A ARPANET, foi responsável pelo início do desenvolvimento da internet, mas foram vários os ajustes responsáveis pelo seu aperfeiçoamento até chegar na sua versão atual.

A internet como é percebida atualmente foi concebida em 1994 com a implementação da World Wide Web (WWW), também conhecida como “WEB”, criado pelo inglês Tim Berners-Lee, no Centro Europeu de Investigação Nuclear (CERN), em Genebra (CASTELLS, 2003). VILHA complementa:

> A web pode ser definida como um conjunto de recursos que possibilita navegar na Internet por meio de textos hipersensíveis com hiper-referências em forma de palavras, títulos, imagens ou fotos, ligando páginas de um mesmo computador ou de computadores diferentes. A web é o segmento que mais cresce na internet e a cada dia ocupa espaços de antigas interfaces da rede. (VILHA, 2002, pág. 20).

Através da WEB, foi possível a transmissão de imagens, vídeos e sons, uma vez que antes desse marco a internet só realizava a transmissão de textos. Dessa forma, surgiu programas capazes de manipular interfaces gráficas, facilitando a comunicação de dados pela internet e a criação de provedores de acesso aos serviços de internet, possibilitando ao público acessá-la.

Devido a sua popularização, a internet foi se expandindo cada vez mais, chegando a um nível global, tendo sua estrutura ampliada e melhorada facilitando seu uso e o seu acesso.

Com os avanços da tecnologia e a criação de novos meios digitais, a internet passou a ser acessada não só por computares, mas também smartphones, televisões, tablets, dentre outros dispositivos.

Conforme o IBGE (Instituto Brasileiro de Geografia e Estatística), em 2017 a Internet era utilizada em 74,9% dos domicílios brasileiros e 98,7% desses domicílios, o smartphone era o meio mais utilizado para acessá-la.

A internet continua sendo passível de transformações, permitindo cada vez mais o desenvolvimento de formas sofisticadas de comunicação e interação. Ademais, acomoda e incentiva a evolução de outras tecnologias, facilitando ainda mais a transmissão de dados, a realização de tarefas e a ampliação de serviços.

1.2 NOÇÕES GERAIS SOBRE CIBERCRIMINALIDADE

A internet é um instrumento de extrema importância no mundo todo, o seu uso trouxe inúmeros benefícios nas mais variadas áreas e atividades e se tornou imprescindível na vida das pessoas.

No entanto, por ser um instrumento de comunicação, transmissão de informações e de dados, e por substituir diversas atividades manuais ou presenciais dos indivíduos por atividades digitais e online, tornou-se também um instrumento de prática de condutas ilícitas perigosas, conhecidos como crimes virtuais/informáticos/cibernéticos.

Relatos apontam que os crimes virtuais começaram a ocorrer na década de 1970, mas apenas no fim dos anos 90, em uma reunião feita pelo G-8, a qual tinha o intuito de discutir sobre as formas de combater os atos ilícitos praticadas na internet, de forma punitiva e preventiva, que se originou o termo “cibercrime”, o qual passou a ser usado para denominar as infrações penais praticadas no ambiente virtual. (D’URSO, 2017).

São várias as denominações utilizadas atualmente para se referir a prática dessas infrações penais, no entanto, a maioria dos autores as definem como “crimes digitais”.

De acordo com CASSANTTI:

> Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital. (CASSANTI, 2014, p. 03)

O autor, ao tratar do assunto, acrescenta: “Crimes virtuais são delitos praticados através da internet que podem ser enquadrados no Código Penal Brasileiro resultando em punições como pagamento de indenização ou prisão.” (CASSANTI, 2016).

Desse modo, os crimes praticados ou potenciados pela via virtual, utilizando a internet ou os sistemas informáticos, podem atentar contra vários tipos de bens jurídicos, especificamente as pessoas (a vida, a honra, liberdade individual, etc.) e o património (material e imaterial).

O doutrinador ROSSINI, aduz que:

> [...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança Informática, que tem por elementos a integridade, disponibilidade a confidencialidade.(ROSSINI, 2004, p. 110.)

Como já demonstrado, os delitos informáticos ocorrem no ambiente virtual, por meio da internet ou sistemas informáticos, sendo praticados não apenas através dos computadores, mas também através das plataformas moveis, tais como celulares, smarthphones, tablets, por meio das mais diversas formas, sendo alguns exemplos: vírus, spam, botnet, phishing, spyware, worm, entre outros.

O cibercriminoso é aquele agente que prática conduta típica, antijurídica e culpável, virtualmente, e será processado, julgado e punido por suas ações. Esses agentes não possuem um perfil padrão, podendo ser tanto pessoas possuidoras de um conhecimento técnico mais profundo a respeito da internet, os chamados hackers ou crackers, quanto usuários comuns que, por meio de seus atos no âmbito virtual praticam os mais variados crimes (estelionato, crimes conta honra, pedofilia, racismo) contra outros usuários.

Os crackers, são conceituados por FELIZARDO como:

> Cracker - expert em computador que tem domínio e habilidade em programações e desenvolvimento de sistemas. Invade o sistema de computação de outra pessoa, ou rede, quebrando palavras-chave, licenças,

> senhas e proteções: age de forma ilegal e sem ética, com intenção de dolo. (FELIZARDO, 2010, p.135)

Assim, entende-se que os crackers são indivíduos que utilizam do seu conhecimento em informática para “quebrar” sistemas de segurança, códigos de criptografia e senhas de acesso a redes, de forma ilícita para fins criminosos.

Existem ainda algumas subdivisões que representam outras habilidades dos crackers, sendo as principais:

Defacer: são experts em deixar sua “marca” em sites, através de mensagens de protesto contra uma causa ou contra o próprio site;

Spammer: espalham e-mails com correntes e vírus que danificam e/ou roubam informações de usuários, desde dados pessoais à dados bancários;

Cyberpunk: causam danos às vítimas por simples forma de prazer, podendo ser pela queda do servidor ou até mesmo pela eliminação completa dos dados armazenados;

Carder ou estelionatários: são especialistas em roubar informações bancarias, como números de cartão de credito;

Phisher: são responsáveis por aplicar os mais diversos golpes contra outros usuários através de links fraudulentos.

Já os hackers, diferente do que muitos pensam, não estão relacionados a furto de dados ou invasão de sistemas. Podem ser definidos como um programador de sistemas e desenvolvedor de proteção e softwares, ou seja, o hacker utiliza todo seu conhecimento técnico para aperfeiçoar softwares licitamente e elaborar soluções inteligentes para um problema de programação e segurança. Destaca NOGUEIRA:

> Este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam desafiar entre si, para ver quem consegue invadir tal sistema ou página da internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual.(NOGUEIRA, 2008, p.52)

Dessa forma, conclui-se que com o aprimoramento e popularização dos meios eletrônicos e surgimento da internet, se tornou cada vez mais frequente a prática de atos delituosos por meio da esfera digital.

Os agentes se utilizam de todos os recursos e meios possíveis proporcionados pela internet e outros instruementos tecnológicos, para cometerem os mais diversos tipos de infrações.

Eles não precisam, inclusive, ter um notório conhecimento de informática, usam do anonimato ou até mesmo do equivocado pensamento de estarem protegidos por uma tela digital para disseminarem ódio, para difamar, ofender, piratear, roubar informações, divulgar dados pessoais de outrem sem a devida permissão, entre outras inúmeros delitos.

Ademais, com o surgimento da esfera obscura mundial de computadores, a “dark web” (parte anônima da deep web), crimes mais graves contra a honra e contra o patrimônio passaram a ser cometidos e planejados, tais como pedofilia, terrorismo, apologia ao crime, comercialização ilegal de produtos, comercialização de armas, tráfico de drogas, entre outros.

A Deep Web é o nome que se dá à zona da internet que não pode ser acessada através de mecanismos de busca, como o Google ou navegadores Chrome, Safari ou o Edge. Por conter conteúdos sigilosos, difíceis de serem acessados e descobertos, passou a ser usado por pessoas perigosas com intuito de praticar condutas criminosas sem serem descobertas.

Assim, muitos indivíduos passaram a utilizar a rede para ferir o direito do outro, com o pensamento de que ali estariam “à salvo da Justiça”, podendo cometer as mais variadas infrações e não serem “pegos”.

No entanto, o Brasil, com a promulgação da Constituição em 1988 que estabeleceu que as questões de informática deveriam ser de competência do Estado, vem tomando medidas para lidar com essa nova realidade, tentando alcançar os infratores no plano virtual e aplicando punições no mundo real.

A legislação brasileira conta com algumas normas, as quais preveem direitos, deveres, sanções quanto ao uso da internet no Brasil. Entretanto, essas normas não acompanham as necessidades sociais e a complexidade que se trata o cibercrime.

2. TIPOS PENAIS NO ÂMBITO CIBERNETICO

Os crimes virtuais, como já mencionado anteriormente, são fatos típicos e antijurídicos cometidos por meio dá, ou contra a tecnologia da informação, ou seja, ato típico e antijurídico, praticados por meio da informática em geral, ou contra um sistema, dispositivo informático ou redes de computadores. (Jesus e Milagre, 2016) São atos ilícitos realizadas por algum tipo de dispositivo tecnológico, isto é, condutas ilícitas praticadas em um ambiente virtual (Rocha, 2017).

Não existe um acordo na doutrina quanto aos crimes praticados através de meios eletrônicos, bem como não há um consenso quanto a sua classificação. Vários doutrinadores, os conceituam como “crimes digitais”, outros como “crimes virtuais” e ainda “crimes cibernéticos”.

Classificar estes crimes no código penal, não é tarefa simples e fácil, posto que, a tecnologia está sempre em evolução, mudando rapidamente e constantemente, o que faz com que as análises e opiniões dos legisladores sobre o assunto também mude frequentemente. Contudo, essa classificação é um tema ainda ativo, realizada tendo como base o bem jurídico tutelado pela lei penal. (FRAGOSO, 1983)

Neste sentido, tem-se ainda que crimes virtuais podem ser classificados como próprios ou impróprios. Os próprios são condutas antijurídicas e culpáveis, cujo objetivo é causar dano a um sistema ou violar seus dados, afetando sua confiabilidade e integralidade.

Os impróprios são condutas comuns, no entanto, típicas, antijurídicas e culpáveis praticadas utilizando-se de mecanismos informáticos como ferramenta, mas que poderiam ter sido praticadas por outros meios, ou seja, poderiam ter sido praticadas fora da esfera virtual, no plano real, como por exemplo, o crime de racismo, discurso ao ódio, crimes contra honra etc. (SYDOW, 2014).

Ademais, os crimes cibernéticos podem ser praticados por uma multiplicidade de agentes, podendo ocorrer, inclusive, mais de uma conduta lesiva ao mesmo tempo, podendo estes criminosos estarem em diversos lugares simultaneamente no ambiente virtual.

Além disso, os agentes contam ainda com o fato de serem, muitas vezes, discretos e silenciosos, e de não terem, comparando com o crime na esfera “real”, local preciso, certo, de fácil acesso pelas autoridades responsáveis.

O cibercrime não se utiliza do contato físico entre vítima e agente, ocorrendo em um ambiente muitas vezes sem pessoas, governo ou território, além de não gerar, a princípio, sensação de violência para um segmento social específico, não havendo padrões para o seu acontecimento (SYDOW, 2009).

Assim, fica mais difícil verificar a ocorrência de uma conduta criminosa na esfera virtual, uma vez, que não é tarefa fácil localizar o agente que a cometeu, além de que, algumas condutas possuem certas peculiaridades o que torna necessário uma maior análise para uma melhor adequação quanto ao seu tipo penal, para que assim, medidas possam ser tomadas.

Neste sentido, em razão da pluralidade de crimes cometidos na esfera virtual, o presente trabalho abordará apenas os principais.

2.1 ESTELIONATO

Os primeiros crimes virtuais eram voltados a sabotar sistemas e tecnologias. No entanto, com a expansão da internet, mais pessoas passaram a utilizá-la, aumentando, assim, a oportunidade para a prática de diferentes crimes (ROCHA, 2017).

Desse modo, os crimes virtuais tiveram uma rápida evolução, saindo das práticas de sabotagens e passando a englobar outras práticas criminosas, como por exemplo, o estelionato virtual, roubo e exposição de informações e de imagens íntimas (FERREIRA, SANTOS E COSTA, 2019).

O estelionato é um crime já conhecido pela sociedade, sendo cometido tanto na esfera virtual, quanto fora dela, e está disposto no artigo 171, do Código Penal.

Atualmente, com o agravamento da pandemia do novo Coronavírus, foi notório o aumento das condutas criminosas praticadas por meio da internet, o que acarretou na criação da PL 4.554/2020, a qual prevê a modalidade qualificada dos crimes de furto e estelionato por meio da internet, com o consequente aumento de pena para referidos delitos, *in verbis:*

> 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 1 (um) a 5 (cinco) anos, e multa.
>
> Fraude eletrônica
>
> § 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.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
> Estelionato contra idoso ou vulnerável
> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso (BRASIL, 2021)

No âmbito virtual, o estelionato é praticado pela conduta do agente de "induzir ou manter a vítima em erro, e com isso, obter vantagem ilícita, para si ou para outrem". Portanto, o objetivo do agente é iludir a vítima, induzi-la ao erro, para que voluntariamente, ela entregue o bem, valores ou informe seus dados pessoais, os quais possibilitará ao agente encontrar formas de obter vantagens nome da vítima.

É muito comum a utilização de links, encaminhados por e-mail, mensagens de texto ou por redes sociais como o Whatsapp, Instagram, com algum conteúdo falso, que serve de "isca" aos usuários.

Assim, o conteúdo induz o usuário a clicar no referido link, direcionando-o a um site falso onde acaba indicando seus dados pessoais e/ou até bancários, possibilitando ao agente apropriar-se desses dados e, posteriormente, transferir valores disponíveis em contas bancárias para o seu domínio ou realizar compras em nome do usuário, vítima desse golpe. Essa modalidade é conhecida como Phishing.

Os e-mails ou mensagens enviadas, geralmente são disfarçadas, como se tivessem sido enviados por agências bancárias alertando sobre compras indevidas ou pedindo a atualização de dados cadastrais, sempre induzindo a vítima a clicar em um link, e posteriormente, fornecer seus dados.

Também pode apresentar arquivos que ao serem baixados, infectam o aparelho com um "*malware"*, que pode furtar os dados ou arruinar todos os arquivos do dispositivo eletrônico.

Outra forma de estelionato é a utilização de sites falsos com a mesma aparência e registro semelhante dos originais, para a captação de dados do usuário. Essa prática é conhecida como Typosquatting (BARRETO, 2021). Por meio dessa modalidade, os agentes estruturam uma página web na internet e registram o domínio idêntico ao de alguma grande empresa conhecida, resultando, por exemplo em: site original – *www.walmart.com*; site falso – www.wallmart.com (BARRETO, 2021).

Dessa forma, a plataforma criada não tem qualquer relação com a verdadeira empresa, e ao inserir os dados, como usuário e senha ou numeração do cartão de crédito, os estelionatários adquirem tais informações para si, e as utilizam, posteriormente.

Atualmente, tem ocorrido muito a clonagem de números telefônicos, o que também configura crime, em que o a gente se passa por algum conhecido da vítima, pedindo dinheiro, induzindo-a a transferir os valores desejados para a conta do criminoso.

Essa prática também ocorre sem a clonagem, em que os criminosos, por meio de outros números telefônicos, se passam por algum conhecido da vítima, com a narrativa falsa de que “perderam ou trocaram de número” e por isso estão falando por um novo e desconhecido.

Dessa forma, nota-se que, a medida em que a internet se expande e as redes sociais e seus sistemas de proteção se aprimoram, novos meios para a execução de crimes virtuais vão sendo criados.

2.2 CRIMES CONTRA A HONRA

Com a expansão da internet e o aperfeiçoamento dos sites e das redes sociais, os indivíduos passaram a se tornar alvo de uma exposição pública maior, tendo sua imagem e privacidade cada vez mais expostas e sua honra atingida.

Honra são as características, particularidades, físicas, morais e intelectuais de um indivíduo, que faz com que ele seja respeitado perante a sociedade. A honra é o que define se o indivíduo será ou não aceito em determinado grupo social, sendo, portanto, um patrimônio pessoal que deve ser protegido (CRESPO, 2011).

Os crimes contra a honra estão previstos nos arts. 138 (calúnia), 139 (difamação) e 140 (injúria), do Código Penal, possuindo uma dimensão muito maior quando praticados na esfera virtual. Salienta-se que, a “honra” nesse diploma, abrange os aspectos objetivos e subjetivos.

A honra objetiva refere-se a opinião de terceiros às características físicas, intelectuais, morais de alguém. O indivíduo tem algo que permeia na sociedade, ou seja, é aquela que se refere a boa índole do sujeito no meio social (CAPEZ, 2019).

Já a honra subjetiva se refere à opinião do indivíduo sobre si mesmo, em suma, diz a respeito da sua autoestima, o que ele pensa de si próprio, o que ele pensa das suas características morais, físicas e intelectuais, não importando a opinião de terceiros (CAPEZ, 2019).

Muitos acreditam que a internet é uma terra sem lei e, devido a maior exposição em que os indivíduos ficam sujeitos, além do fato de muitos usuários usarem do anonimato ou acharem que podem se esconder através de uma conta nas redes sociais, fica cada dia mais frequente a prática de crimes contra a honra no âmbito virtual.

O crime de difamação é um dos crimes contra a honra e está definido no artigo 139 do código penal: Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena – Detenção, de 3 (três) meses a 1 (um) ano, e multa.

Consiste em atribuir a alguém fato determinado ofensivo à sua reputação, sendo esse fato verdadeiro ou não. Assim, no crime de difamação não se exige que a atribuição que foi feita ao indivíduo seja falsa, bastando apenas que o agente sinta que sua honra foi ferida, ofendida perante a sociedade, diante da a atribuição que lhe foi feita.

Dessa forma, o crime se consuma quando terceiro toma conhecimento do fato atribuído ao indivíduo. Na esfera virtual, esse crime se consuma quando houver divulgação, nas redes sociais por exemplo, de um fato considerado ofensivo, a respeito de um determinado indivíduo.

Portanto, é um crime que ataca a honra objetiva da pessoa humana, não podendo ser sujeito passivo a pessoa jurídica, devendo nesse caso ser aplicado lei nº 5.250/67 – Lei de Imprensa INELLAS (2004).

O crime de calúnia está definido no art. 138 do Código Penal Brasileiro, epsis verbis: “Caluniar alguém, imputando-lhe falsamente fato definido como crime” e

segue ainda no § 1º, determinando que "na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga".

Assim, no crime de calúnia, o agente imputa a alguém o cometimento de um crime, sendo essa alegação falsa e tendo o agente conhecimento da falsidade dessa alegação, ferindo, consequentemente, a honra objetiva da vítima, sua reputação frente a sociedade.

No ambiente virtual, esse crime se consuma quando um indivíduo imputa um crime a outrem, por meio de comentários, postagens, fotos, vídeos nas redes sociais.

Qualquer indivíduo pode ser considerado sujeito ativo no crime de calúnia, bem como pode qualquer pessoa ser sujeito passivo. Nos termos do art.138, § 2º, do Código Penal, até os mortos podem ser caluniados, sendo que neste caso os sujeitos passivos serão os seus familiares vivos.

Quanto a possibilidade de pessoas jurídicas serem consideradas sujeito passivo, ainda há divergências jurisprudências e doutrinarias sobre o assunto, Julio Fabrini Mirabete, preleciona:

> Apenas pode ser uma pessoa física, pois empresas e outras entidades não podem cometer crimes e, portanto, não podem ser falsamente acusadas do crime, porém pode acontecer que a acusação feita a uma empresa possa acabar indiretamente recaindo sobre seus administradores. (MIRABETE, Júlio Fabrini, 2006, p.29)

Contudo, com a Lei n. 9.605/98, a qual prevê os crimes contra o Meio Ambiente, tornou-se possível caluniar pessoa jurídica, por meio de imputação falsa quanto a prática de crime ambiental.

Já o crime de injúria está previsto no art. 140 do Código Penal Brasileiro, *ipsis verbis*: "Injuriar alguém, ofendendo-lhe a dignidade ou o decoro".

Deste modo, o agente atribui qualidade negativa a vítima, qualidade esta que diga respeito as suas características, particularidades, morais, físicas ou intelectuais, ofendendo de forma subjetiva a honra da vítima, ou seja, ofendendo a sua dignidade ou o decorro.

Portanto, diferente da calúnia e da difamação, a injúria é uma atribuição de uma qualidade negativa da vítima e não de um fato determinado e a sua consumação ocorre quando a vítima toma conhecimento da ofensa.

No ambiente virtual, esse crime é praticado por comentários, mensagens e postagens do agente ofendendo a vítima com atribuições negativas sobre suas características morais, físicos, intelectuais.

O sujeito ativo, bem como o sujeito passivo, podem ser qualquer pessoa física, não se admitindo pessoas jurídicas, pois essas, não possuírem honra. (PRADO, 2006)

2.3 PORNOGRAFIA INFANTIL

Nos últimos anos o Brasil avançou na luta contra os crimes praticados contra a dignidade sexual na internet. Criou-se dispositivos úteis ao enfrentamento destes crimes, tanto na esfera processual quanto na penal (BARRETO, 2021).

A pornografia infantil é uma conduta criminosa, um tipo de violência sexual cometida contra vulneráveis (criança e adolescentes), que acabou ganhando força com a atual facilidade de acesso à internet. A prática desse crime está tipificada no Estatuto da Criança e do Adolescente (ECA), e no Código Penal, assim como também na Convenção dos Direitos da Criança da ONU, de 1989.

Os artigos 240 a 241-E, do ECA, descrevem as condutas que tipificam a pornografia infantil, visando criminalizar a aquisição e a posse de tal material, bem como, combater à produção, venda e distribuição de pornografia infantil.

O art. 240, salienta ser crime contra vulneráveis as seguintes condutas:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa

Ademais, a pornografia infantil não é praticada apenas por aqueles que querem prazer próprio, é praticado também por aqueles que visam lucro com a criação e comercialização de material pornográfico.

Neste sentido, dispõe o artigo 241, do ECA:

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

Ainda, aquele que de alguma maneira compartilha, troca, publica, divulga, oferece, possui ou armazena, bem como, simula (por adulteração, montagem,

modificação) a participação de crianças ou adolescentes em cenas de conteúdos pornográficos, mesmo que sem intenção lucrativa, também concorre a sanções estabelecida pelo ECA, conforme seus artigos 241- A, 241-B e 241-C.

Esse crime aumentou drasticamente com a expansão da internet e criação da deep web, a qual não será abordada amplamente no presente trabalho, mas em suma trata-se de uma plataforma quase não conhecida pela população, de difícil acesso e que permite a prática de condutas ilícitas por meio de sites considerados "invisíveis", uma vez que, não aparecem nos mecanismos de busca tradicionais como o Google.

Por meio dessa plataforma são praticados os mais diversos crimes, o que dificulta ainda mais o trabalho das autoridades em descobrir os agentes dessas condutas, posto que, o acesso a deep web é complexo e os agentes se escondem através do anonimato.

A jurisprudência é dura na aplicação das penas envolvendo essas condutas, podendo ser destacado a decisão do Superior Tribunal de Justiça, a qual estabelece que quando praticado na internet tem caráter transnacional. Veja-se:

> HABEAS CORPUS Nº 413.069 - SP (2017/0208680-6) RELATOR: MINISTRO JOEL ILAN PACIORNIK IMPETRANTE: DEFENSORIA PÚBLICA DA UNIÃO ADVOGADO: DEFENSORIA PÚBLICA DA UNIÃO IMPETRADO: TRIBUNAL REGIONAL FEDERAL DA 3A REGIÃO PACIENTE: MICHAEL LEME DE QUEIROZ DECISÃO Cuida-se de habeas corpus substitutivo de recurso próprio, com pedido de liminar, impetrado em benefício de MICHAEL LEME DE QUEIROZ, contra acórdão do Tribunal Regional Federal da 3ª Região (APC n. 2016.61.14.002516-6). Consta dos autos que o paciente foi condenado em primeiro grau pela prática dos crimes do 20 arts. 241-A e 241-B, do Estatuto da Criança e do Adolescente c.c. art. 69 do Código Penal, à pena de 4 (quatro) anos de reclusão, em regime aberto, consistentes em prestação de serviços à comunidade e prestação pecuniária. O Tribunal Regional Federal da 3ª Região, por sua vez, negou provimento ao recurso defensivo e deu parcial provimento ao recurso ministerial, conforme ementa a seguir transcrita: DIREITO PENAL. PROCESSO PENAL APELAÇÕES CRIMINAIS. PORNOGRAFIA INFANTO-JUVENIL. LEI 8.069/90. ARTIGOS 241-A E 241-B. PROGRAMA DE COMPARTILHAMENTO DE DADOS. USO. COMPETÊNCIA. JUSTIÇA FEDERAL. DOLO CARACTERIZADO NO COMPARTILHAMENTO DOS ARQUIVOS ILÍCITOS. AUTORIA E MATERIALIDADE INCONTROVERSAS. ABSORÇÃO. INOCORRÊNCIA NO CASO CONCRETO. CONDENAÇÃO MANTIDA. DOSIMETRIA. ALTERAÇÕES. 1. Réu flagrado em posse de acervo de fotografias e vídeos de pornografia infantojuvenil, acervo este armazenado digitalmente em discos rígidos de sua propriedade. Teria, ainda, compartilhado arquivo do mesmo teor anteriormente. [...] Em outros termos: ao disponibilizar arquivos de conteúdo pornográfico infanto-juvenil em servidor mundialmente acessível, o que há é a disponibilização/divulgação de pornografia infanto-juvenil além das fronteiras nacionais, o que torna claro seu caráter transnacional. [...] 3. Por sua vez, a constatação da internacionalidade do

> delito demandaria apenas que a publicação do material pornográfico tivesse sido feita em "ambiência virtual de sítios de amplo e fácil acesso a qualquer sujeito, em qualquer parte do planeta, que esteja conectado à internet" e que "o material pornográfico, envolvendo crianças ou adolescentes tenha estado acessível por alguém no estrangeiro, ainda que não haja evidências de que esse acesso realmente ocorreu" [...] Publique-se. Intime-se. Brasília (DF), 23 de fevereiro de 2018. (STJ - HC: 413069 SP 2017/0208680-6, Relator: Ministro Joel Ilan Paciornik, Data de Publicação: DJ 28/02/2018)

O Superior Tribunal Federal, ainda estabelece que a mera divulgação do conteúdo sexual envolvendo os vulneráveis já se consuma o crime de pornografia infantil. *In verbis:*

> Primeira turma do STF: ESTATUTO DA CRIANÇA E DO ADOLESCENTE – Art. 241 – Inserção de cenas de sexo explícito em rede de computadores (Internet) – Crime caracterizado – Prova pericial necessária para apuração da autoria. “Crime de computador”; publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores atribuída a menores – Tipicidade – Prova pericial necessária à demonstração da autoria – Habeas Corpus deferido em parte. 1. O tipo cogitado – na modalidade de “publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente” – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma normal aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta incriminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da Lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada do conhecimento do homem comum, impõe se a realização de prova pericial.

Destarte, a pornografia infantil é um crime doloso, o qual exige-se apenas o dano potencial, não necessitando de dano material efetivo para ser consumado, tendo como objeto material a foto, o vídeo ou a imagem contendo pornografia ou sexo explícito envolvendo criança ou adolescente e, ainda, tendo como objeto jurídico a proteção à formação moral da criança ou adolescente (NUCCI, 2016).

Ainda, nos termos do art. 241-A, parágrafo 2º, a autoridade policial ou Ministério Publico podem oficiar o responsável técnico dos sites os quais contenham fotos, vídeos ou qualquer outro registro que tenha sexo explícito ou pornografia envolvendo menores, requisitando sua remoção em 24 horas, sob pena de 03 a 06 de reclusão e multa.

Além disso, a solicitação também pode ser feita pelos pais ou representantes da vítima, e em caso de descumprimento recomenda-se a instauração de inquérito e posterior indiciamento do investigado (BARRETO, 2021).

3. OS REFLEXOS DOS CRIMES VIRTUAIS NO DIREITO BRASILEIRO – ATUALIDAES

Como já abordado, a popularização da internet trouxe inúmeros benefícios, contudo, diante da facilidade de acesso por qualquer pessoa e da sua dimensão, sendo inclusive considerada uma “terra sem lei”, a internet acabou gerando também inúmeros empecilhos.

Os órgãos judiciais e investigativos enfrentaram dificuldades em identificar os sujeitos ativos dos crimes praticados nos ambientes virtuais, em virtude das particularidades e inovações dos meios tecnológicos e da internet, que acabaram facilitando a fuga e a ocultação de autoria. Isso ocorre, sobretudo, em razão do “*grande número de usuários dessa nova tecnologia e a possibilidade de colocar informações inverídicas sore seu endereço de IP”* (SIQUEIRA, 2017, pág. 122).

Preleciona Siqueira:

> Seria possível a identificação do criminoso obtendo o seu endereço de IP, login e senha do aparelho utilizado para a prática do crime, porém, os criminosos utilizam endereços falsos, dificultando o trabalho investigativo dos policiais. (SIQUEIRA, 2017, pág.122)

É compreensível a dificuldade de investigar e criar leis para o combate dos crimes virtuais, posto que, ainda é tudo muito atual e inconstante, a tecnologia está sempre em mutação e novas condutas ilícitas vão aparecendo nesse meio.

Ressalta-se que, a princípio, os crimes cometidos na esfera virtual eram tipificados por analogia em tipos penais comuns. Assim, era como se a conduta praticada no ambiente virtual ocorresse de modo análogo à conduta enquadrada no tipo comum (TAVARES, 2012).

No entanto, diante dos recorrentes casos de crimes cibernéticos, cujo agentes iam aperfeiçoando cada vez mais os métodos utilizados para as práticas dessas condutas, fazendo ainda mais vítimas, fez-se necessário a criação de novas leis, específicas para o ambiente digital, as quais regulariam esses recentes hábitos, fazendo com que a esfera virtual não ficasse desprovida da tutela jurídica do Estado.

As primeiras medidas legislativas no Brasil, abrangendo o âmbito virtual, ocorreu por meio do Plano Nacional de Informática e Automação, a qual se realizou

por meio da Lei 7.232 de 1984, que abordava a respeito dos preceitos de informática em território pátrio.

Em 18 de dezembro de 1987, foi publicada a Lei 7.646, a qual foi, posteriormente, revogada pela Lei 9.609 de 1998, que introduziu considerações inovadoras sobre a tecnologia virtual.

A nova lei versava sobre a proteção da propriedade intelectual, autoria e registro, dos programas de computadores, das garantias aos usuários de programas de computador, de contratos de licença de uso, sua comercialização no Brasil e sendo a primeira a especificar em seu ordenamento, tipificação notadamente voltada às infrações de informática.

A lei ainda dispôs, sutilmente, sobre a investigação dos delitos, das possíveis diligências e questões processuais. O tipo penal previsto pela Lei 9.609/1998, tem a seguinte redação:

> Art. 12. Violar direitos de autor de programa de computador:
> Pena - Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
>
> Pena - Reclusão de um a quatro anos e multa.
>
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

Em seguida, foi criada a Lei 9.610/1998, complementando a Lei 9.609/1998, dispondo amplamente acerca dos direitos autoriais, aplicando-se a tudo que foi omisso na redação da Lei 9.609/98 (SIQUEIRA, 2017).

Ainda há outras leis, medidas provisórias, decretos, portarias e resoluções que abordam o tema, no entanto, nem todas serão aprofundadas no presente trabalho por não possuírem tanta relevância.

3.1 MARCO CIVIL DA INTERNET

Em 1999 foi apresentado o Projeto de Lei 84/99 no Senado, de autoria do ex-deputado Luiz Piauhylino e relatoria de Eduardo Azeredo, conhecido como Projeto de Lei Azevedo, que dispunha sobre os crimes cometidos na internet e suas penalidades.

Contudo, por ter um caráter “criminalizador”, “vigilista” e repressivo, que violava direitos fundamentais dos usuários, o projeto foi rechaçado pela sociedade e recebendo a alcunha de “AI-5 Digital” (MILAGRE, 2009).

Diante da necessidade de normatizar a internet sem ofender direitos e liberdades, em 29 de junho de 2009, através de um processo de construção colaborativa e democrática entre sociedade e governo, apresentado pela Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL/MJ) em parceria com a Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas e realizado por meio da internet, foi introduzido as bases para o Marco Civil, que resultou no projeto de Lei nº 2.126/11.

Após um longo período de tramitação e algumas alterações, o Projeto de Lei nº 2.126/11 foi aprovado, na Câmara dos Deputados em 25 de março de 2014 e no Senado em 22 de abril do mesmo ano, tornando-se lei sob o nº 12.965/14, sancionada pela ex-presidente Dilma Rousseff em 23 de abril de 2014, e passando a viger em 23 de junho de 2014 .

Assim, com a Lei 12.965/14 surge o Marco Civil da Internet, estabelecendo *“*os princípios, garantias, direitos e deveres para o uso da internet no Brasil bem como diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios nesta matéria” (BRASIL, 2014, online).

Siqueira et al (2017), aduz que:

> 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 assuntos 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 et al, 2017, p. 126)

A lei do Marco Civil tem com intenção proteger a privacidade do usuário na internet buscando assegurar a inviolabilidade e o sigilo das comunicações conforme determina a CR/88 em seu artigo 5º inciso X. *In verbis:*

> 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

A referida lei é conhecida como a “Constituição da Internet” e o seu texto, é composto por 32 (trinta e dois) artigos, organizados em cinco capítulos.

A Lei estabelece que os provedores não podem violar os direitos dos indivíduos à intimidade e privacidade dos usuários, sendo vedado, para tanto, a monitoração dos dados compartilhados pela rede, bem como realizar a divulgação destes. Ademais, assegura a exclusão dos dados quando as partes encerram com as atividades, conforme dispositivos abaixo colacionados:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: (...)
> II - proteção da privacidade;
> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
> Art. 11º Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. (...)
> § 3o Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. (BRASIL, 2014)

Maia (2017), afirma que o Marco Civil se assenta em três pilares: “a garantia da neutralidade da rede; proteção à privacidade do usuário da Internet; e a garantia da liberdade de expressão”.

A neutralidade da Rede procura oferecer uma democratização do acesso à Internet, garantindo que as operadoras não cobrem de forma diferenciada a depender do conteúdo que circula na rede, podendo a mesma cobrar apenas em relação às velocidades oferecidas.

Quanto à privacidade do usuário a lei procura proteger os seus dados junto aos provedores, de modo que apenas em momentos específicos e de extrema necessidade, com ordem judicial, possa haver quebra do sigilo desses dados. Já a liberdade de expressão tem a intenção de impedir a censura (LISBOA, LOPES, 2016).

A regulamentação do marco civil foi de extrema relevância, uma vez que, houve o estabelecimento de prazos mínimos para o armazenamento de registros de acesso e conexão, além de passar a ser obrigatório a observância da lei brasileira para atos realizados no território nacional.

Assim, com o Marco Civil da Internet, a privacidade, a honra, a dignidade e intimidade dos usuários da internet passaram a ter um cuidado maior, visando garantir sua proteção também no ambiente digital.

3.2 LEI CAROLINA DIECKMANN – LEI 12.737/2012

É notório que a evolução da internet é constante e a legislação brasileira deve acompanhar esse ritmo, a fim de regular as garantias e os direitos constitucionais, que acompanham esse avanço tecnológico.

Contudo, mesmo diante das mais diversas e reiteradas formas de praticar o cibercrime, o que se teve inicialmente foi adaptações nos meios digitais, com a criação e uso de senhas e softwares para proteger os usuários de possíveis condutas criminosas no ambiente digital, para só depois se avançar na criação de uma legislação específica.

Assim, como inclusive já destacado, em razão da ausência de uma lei própria para os crimes virtuais, os magistrados, nos casos concretos, se utilizavam do próprio Código Penal para a tipificação, o que dava margem a decisões contraditórias (PAGANOTTI, 2013).

Em decorrência de alguns episódios em meados de 2011, ocorrendo vários ataques na navegação de serviços nos sites do governo brasileiro que ficaram instáveis até saírem do ar, bem como, nos inúmeros outros casos de atos criminosas no âmbito virtual, foi apresentado um novo projeto de lei, em 29 de novembro de 2011 na Câmara dos Deputados.

Esse projeto era de autoria dos Deputados Federais Paulo Teixeira, Luiza Erundina, Manuela D'Ávila, João Arruda, Brizola Neto e Emiliano José, e visava a necessidade de criar uma legislação que regulamentasse de forma mais especifica o uso "criminoso" dos meios cibernéticos, dispondo o seguinte:

> São inegáveis os avanços para a sociedade decorrente do uso da Internet e das novas tecnologias. Estes avanços trazem a necessidade da regulamentação de aspectos relativos à sociedade da informação, com o intuito de assegurar os direitos dos cidadãos e garantir que a utilização destas tecnologias possa ser potencializada em seus efeitos positivos e minimizada em seus impactos negativos. (BRASIL, 2011, D)

Os autores defendiam que as antigas propostas de criminalização, trazidas por outros projetos, eram muito abertas e desproporcionais, não sendo capazes de

aplicar a tipificação criminal de condutas corriqueiras praticadas pelos usuários da internet, bem como, tipificavam matérias como o armazenamento e acesso a registros de conexão, que deveriam estar inseridos em diretrizes mais abrangentes e atentas aos direitos dos cidadãos (BRASIL, 2011).

Assim, o Projeto de Lei nº 2.793 de 2011, apresentou algumas diferenças em relação ao Projeto nº 84/99 (Lei Azeredo) já abordado anteriormente, tais como: trata-se apenas de tipificações penais e apresenta um número significativo menor de tipos penais, veja-se:

> [...] não se abordam as questões relativas a guarda e fornecimento de registros, ou demais obrigações imputáveis a provedores de serviços de internet - questões que encontram lugar mais adequado numa regulamentação civil sobre a matéria. (BRASIL, 2011, D).
> [...] Norteamo-nos, nesta escolha, pela compreensão de que grande parte das condutas relativas praticadas por meios eletrônicos já se encontra passível de punição pelo ordenamento jurídico pátrio. Ainda, pautamo-nos pela visão de que não é a proliferação de tipos penais que levará à maior repressão de condutas. (BRASIL, 2011, D).

Desse modo, a PL buscou excluir as condutas que não eram claras e precisas e, visava uma forma de equilibrar as penas de acordo com a gravidade das condutas e ainda estabelecer uma harmonia com as penas já existentes no Código Penal, bem como, pretendia evitar a expansão desnecessária para novas searas penais (BRASIL, 2011).

Portanto, a sua aprovação seria uma forma de preencher as lacunas presentes na legislação brasileira atual sobre a temática, com o intuito de tentar acompanhar a expansão constante da tecnologia e combater as condutas criminosas praticadas no âmbito digital.

Em 07 de novembro de 2012 foi aprovado o Projeto de Lei, nº 2.793 de 2011, que passou a ser conhecida como “Lei Carolina Dieckmann”, a Lei nº 12.737 de 30 de novembro de 2012, entrando em vigor apenas no dia 02 de abril de 2013.

A promulgação da Lei 12.737/12 e a sua rápida tramitação se deu por conta de um caso de repercussão nacional, envolvendo a atriz brasileira Carolina Dieckmann.

Os portais de notícias e as redes sociais contribuíram para a ampla disseminação desse caso, alcançando um enorme número de pessoas em todo o país e de forma célere.

A atriz teve seu computador invadido por criminosos, os chamados crakers, após receber um e-mail que julgava ser confiável. Assim, os criminosos tiveram acesso a fotos intimas de Carolina, passando a chantageá-la, exigindo R$ 10.000,00 (dez mil reais) para não divulgar as imagens.

A atriz recebeu inúmeras ligações e mensagens, ameaçando-a sobre a divulgação, mas não cedeu as chantagens e registrou boletim de ocorrência na delegacia.

Contudo, a operação montada pela polícia para prender os agentes em flagrante restou frustrada e, segundo o site de notícias da Globo (G1) (http://www.g1.globo.com), “ao todo, 36 imagens intimas da atriz foram pulicadas na web em maio de 2012”.

Diante de toda repercussão do caso, através da mídia e da internet, bem como do medo e insegurança que tal fato gerou aos indivíduos, que se sentiram vulneráveis e suscetíveis a passar pelas mesmas situações, o Congresso Nacional foi pressionado a criar e publicar uma lei específica para os crimes cibernéticos.

Assim, o Congresso, para acalmar o clamor popular da época, no intuito de demonstrar uma rápida resposta para o problema em questão, aprovou o Projeto de Lei 2.793/11, criando a lei 12.737/2012 que passou a ser denominada como Lei Carolina Dieckmann.

A inovação legislativa trazida pela Lei 12.737/2012, introduziu no Código Penal brasileiro o tipo nominado “Invasão de dispositivo informático”, acrescentando os artigos 154-A, e 154-B, e ainda alterou o texto dos artigos 266 e 298, inserindo os crimes praticados via meios informáticos na legislação penal. Assim o texto legal possui a seguinte redação.

> LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.
> Dispõe sobre a tipificação criminal de delitos informáticos; altera o DecretoLei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
> A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:
> 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: “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 obtidas.
> § 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."
> "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."
> 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)
> Art. 4o Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.
> Brasília, 30 de novembro de 2012; 191o da Independência e 124o da República. DILMA ROUSSEFF / José Eduardo Cardozo (BRASIL, 2012, F)

Dessa forma, foi incorporado ao ordenamento jurídico brasileiro, a previsão de crime de invasão de dispositivo alheio, sem motivo ou sem o consentimento do dono, com penalidade de 3 meses a um ano, e com causa de aumento, caso tal invasão causasse prejuízos econômicos à vítima, ou caso se trata-se da administração pública no polo passivo.

O bem jurídico tutelado referia-se à violação da liberdade do usuário do dispositivo informático, através de outro dispositivo informático (NUCCI, 2014). É crime comum, o qual pode ser praticado por qualquer pessoa, não se exigindo uma qualidade ou condição especial do agente para ser sujeito ativo, ou seja, não necessita que o invasor seja um especialista, conhecido como hacker (JUNIOR, 2013, NUCCI, 2014).

Ademais, o sujeito passivo também pode ser qualquer pessoa que seja responsável pelo bem jurídico que foi violado (NUCCI, 2014) seja ele o proprietário ou detentor do bem, como nos casos de equipamentos fornecidos por empresas aos seus funcionários (PRADO, 2013).

Para sua caracterização é fundamental o dolo (não cabendo, portanto, a forma culposa) e o especial fim de agir que é “a obtenção, a adulteração ou a destruição de dados ou informações, também a obtenção de vantagem ilícita” (REIS, 2014).

No entanto, no ano de 2021, a Lei sofreu alterações, mais especificamente pela Lei 14.555/2021, a qual será abordada posteriormente no presente trabalho.

3.3 LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) foi sancionada em 2018 e entrou em vigor apenas no ano de 2020.

Foi inspirada pela GDPR (***General Data Protection Regulation)*** da União Europeia, e tem como objetivo “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.” (Brasil, 2020, online)

Essa lei pretende estabelecer uma segurança jurídica, através de uma regulamentação e condutas para proteger dados pessoais de todos os indivíduos que estejam em território brasileiro, observando os preceitos existentes internacionais.

Para Somadossi:

> A LGPD cria uma regulamentação para o uso, proteção e transferência de dados pessoais no Brasil, nos âmbitos privado e público, e estabelece de modo claro quem são as figuras envolvidas e quais são suas atribuições, responsabilidades e penalidades no âmbito civil – que podem chegar a multa de 50 milhões de reais por incidente. (SOMADOSSI, Henrique. 2018, online)

A lei, portanto, cria uma regulamentação referente a proteção de dados, definindo o que são os dados pessoais, estabelecendo, ainda, quais são os dados sensíveis e os de maior proteção, sendo estes os relacionados a crianças e adolescentes.

A fiscalização e aplicação de penalidades quanto ao descumprimento da LGPD, é feita pela Autoridade Nacional de Proteção de Dados Pessoais, a ANPD, sendo necessário também agentes de tratamento de dados, os quais tem suas funções estipuladas pela própria Lei de Proteção de Dados (Brasil, 2020, online).

Quanto a esfera criminal, a Lei optou por nada dispor, sendo necessário a criação de um Anteprojeto de Lei (LGPD Penal), criado em 2019 por uma comissão de juristas.

O principal objetivo e desafio do anteprojeto é conciliar a privacidade com a persecução penal, de maneira que fique claro o que pode ser usado e compartilhado pelas autoridades estatais nas investigações criminais e na segurança pública, bem como, garantir proteção aos indivíduos para que não tenha seus dados usados de forma descontrolada por essas autoridades (Análise, 2021, online).

Dessa forma, espera-se o máximo de transparência e cuidado em sede de investigação criminal e segurança pública no tratamento de dados pessoais, o que ainda tem que ser muito bem estudado e planejado.

3.4 INOVAÇÕES NA LEGISLAÇÃO NO ANO DE 2021– PANDEMIA DO NOVO CORONAVIRUS

É certo que os crimes virtuais vêm sendo aprimorados a cada dia, sendo criadas novas formas de praticá-los. Assim, o número de casos e vítimas aumentou expressamente, principalmente no atual cenário pandêmico do Novo Coronavírus, o qual atingiu o mundo todo de “surpresa”, mudando completamente a rotina dos indivíduos e os meios de operar as mais diversas atividades.

De um dia para o outro, as pessoas se viram tendo que modificar e aprimorar os meios de exercer suas profissões, negócios, atividades, tiveram que diversificar seus estilos de vida, de modo que não precisassem sair de casa.

A forma mais apta para essa mudança era por meio da internet, uma vez que, diante do isolamento, a ferramenta de trabalho, de estudos, o entretenimento e a forma de estar em contato com o “mundo lá fora”, se dava por meio dela.

Dessa forma, a internet passou a ser muito mais utilizada, havendo um aumento exorbitante nos usos das redes sociais, e consequente, elevando o número de casos de cibercrimes.

Nesse sentido, muitos projetos de leis caminharam a fim de tipificar diversas condutas delitivas relacionadas a tecnologia da informação, majorar algumas, qualificar outras.

3.4.1 Lei de Stalking

No dia 31 de março de 2021 foi sancionada a lei 14.132/21, conhecida como Lei de Stalking, uma importante inovação legislativa que incluiu o artigo 147-A no Código Penal, criminalizando a conduta de perseguição, em inglês stalking. Veja-se:

> 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.
> § 3º Somente se procede mediante representação."

Conforme prelaciona Castro e Sydrow (2017) “stalking é uma palavra inglesa aplicada a quem importuna de forma insistente e obsessiva uma outra pessoa, ou seja, a atitude de espionar e perseguir um individuo de forma constante é denominada de stalking”.

Nesse sentido, os autores acrescentam: "trata-se de curso de conduta de importunação, caracterizado pela insistência, impertinência e habitualidade, desenvolvido por qualquer meio de contato, vigilância, perseguição ou assédio."

O delito possibilita que a perseguição também ocorra no meio digital, geralmente com o uso das redes sociais, passando a ser denominado como cyberstalking.

Neste sentido, o projeto de Lei que visa a criminalização dessas condutas foi apresentado pela Senadora Leila Barros, em novembro de 2019, sob a narrativa de que:

> O avanço das tecnologias e o uso em massa das redes sociais trouxeram novas formas de crimes, sendo necessário o aperfeiçoamento do Código Penal para dar mais segurança às vítimas de um crime que muitas vezes começa on-line e migra para perseguição física". (BRASIL, 2021).

O projeto então foi sancionado pelo Presidente Jair Bolsonaro em março de 2021, entrando em vigor no dia 1º de abril do mesmo ano.

Antes, essa conduta era enquadrada apenas como contravenção penal (o (Artigo 65 da Lei de Contravenções Penais - Decreto-Lei 3.688, de 1941), a qual foi revogada e previa como perturbação da tranquilidade alheia, punível com prisão de 15 dias a 2 meses e multa.

Ressalta-se que, a perseguição para ser criminalmente relevante, exige reiteração, de modo a consistir, posteriormente em outro delito, tal como constrangimento ilegal ou ameaça, prejudicando a integridade física ou psicológica da vítima, abalando seu estado emocional e gerando receio ou intranquilidade (BARRETOS, 2021).

Conforme Castro e Sydow (2017) "trata-se, portanto, de um crime habitual, em razão da exigência de atos reiterados para consumação. Assim, uma conduta isolada do agente não é capaz de configurar o crime, razão pela qual, não se admite a tentativa".

Ademais, pode ser cometido por qualquer pessoa, seja homens ou mulheres, prevendo a legislação aumento de pena em metade, se caso ocorre com o concurso de agentes ou no caso de uso de armas.

Também terá pena aumentada em 50% quando for praticado contra criança, adolescente, idoso ou contra mulher por razões de gênero.

A forma de consumação pode ser vinculada, uma vez que, o próprio tipo penal prevê "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" (BRASIL, 2021).

Destarte, "a perseguição reiterada na internet, ameaçando a integridade física e psicológica de alguém, interferindo na liberdade e na privacidade da vítima, configuram cyberstalking" (BRASIL, 2021).

Salienta-se que, as penas desse crime, não afastam as penas correspondentes à violência, o que gera maior proteção às vítimas e proporciona uma aplicação mais integral da lei penal (BARRETOS, 2021).

3.4.2 Alterações no Código Penal e Processual Penal no ano de 2021

Como já mencionado, no final de maio de 2021, o governo federal sancionou a Lei 14.155/2021, alterando alguns dispositivos do Código Penal.

Com essa lei, os crimes cibernéticos como invasão de dispositivo, fraude, furto e estelionato praticados com o uso de dispositivos eletrônicos como celulares, computadores, tablets, etc, ocorridos na esfera digital, conectado ou não à internet, passaram a ser punidos com penas mais duras, gerando, ainda que pouco, uma maior proteção aos usuários da internet.

Conforme pondera Luiz Augusto D'Urso, especialista em Direito Digital, *"*Agora, a invasão de dispositivo informático (art.154 -A, CP) implica reclusão de um a quatro anos, enquanto o furto mediante fraude pela internet e o estelionato pela internet ou pelas redes sociais têm, cada um, pena de reclusão de quatro a oito anos.*"*

Nesse sentido, com a referida Lei, se torna crime a violação de dispositivo informático mesmo que o mecanismo de segurança não seja violado. Ainda, caso não seja preciso a violação desse mecanismo de segurança para ter acesso ao dispositivo, a não autorização do responsável juntamente com o dolo de obter, destruir ou adulterar do agente, já configura um cibercrime.

Dessa forma, as empresas que deixarem público dados pessoais de seus usuários, mesmo que por erro, sofreram punições.

Conforme a nova redação do Código, estabelece o Senado Federal:

> A invasão de dispositivo informático passará a ser punido com reclusão, de um a quatro anos, e multa, aumentando-se a pena de um terço a dois terços se a invasão resultar em prejuízo econômico. Antes, a pena aplicável era de detenção de três meses a um ano e multa.

> A penalidade vale para aquele que invadir um dispositivo a fim de obter, adulterar ou destruir dados ou informações sem autorização do dono, ou ainda instalar vulnerabilidades para obter vantagem ilícita.
> Já se a invasão provocar obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou o controle remoto não autorizado do dispositivo invadido, a pena será de reclusão de dois a cinco anos e multa. Essa pena era de seis meses a dois anos e multa antes da sanção da nova lei.
> Na pena de reclusão, o regime de cumprimento pode ser fechado. Já a detenção é aplicada para condenações mais leves e não admite que o início do cumprimento seja no regime fechado. (BRASIL, 2021)

A inovação legislativa também trouxe novas tipificações para o art. 155 e 171, do Código Penal. Veja-se:

> Art.155.....
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I - aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II - aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.
> Art.171 .....
> Fraude eletrônica
> § 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.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
> .....
> Estelionato contra idoso ou vulnerável
> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.
> .....
> Art. 2º O art. 70 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido do seguinte § 4º:
> Art.70 .....
> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção." (BRASIL, 2021)

Desse modo, ressalta-se que, no crime de furto mediante fraude, o agente coleta os dados bancárias da vítima e furta o dinheiro de sua conta através de transferências.

A nova redação acrescenta “agravante do furto qualificado por meio eletrônico, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento similar, em que a pena será de reclusão de quatro a oito anos e multa*”* (BRASIL, 2021).

Ainda, “se for praticado contra idoso ou vulnerável, a pena aumenta de um terço ao dobro e se for praticado com o uso de servidor de informática mantido fora do país, o aumento da pena poderá ser de um terço a dois terços” (BRASIL, 2021).

No crime de estelionato, a nova Lei “majorou a pena para quatro a oito e multa quando a vítima for enganada e fornecer informações por meio de redes sociais, podendo ser aumentada se for utilizado servidor fora do território nacional ou se o crime for praticado contra idoso ou vulnerável” *(*BRASIL, 2021).

Estabeleceu, ainda, que se praticado por meio de depósito, emissão de cheques sem fundos ou mediante transferência de valores, a competência será definida pelo local do domicílio das vítimas.

Neste sentido, pondera Alexandre Gonçalves Barreto:

> Destacamos a importância de bem diferenciar o crime de furto mediante fraude do delito de fraude eletrônica. A melhore maneira para isso é analisar o elemento comum a ambos: a fraude. No furto ela é utilizada pelo cibercriminioso com o fito de burlar a vigilância da vítima, facilitando a subtração. Desse modo, a vítima não entrega o bem por espontânea vontade. Já na fraude eletrônica, modalidade de estelionato, a fraude visa obter o consentimento da vítima que, ludibriada, entrega voluntariamente o bem. (BARRETOS, 2021, p.136)

Além disso, com a nova Lei, houve mudanças também no âmbito processual penal, impedindo a troca de reclusão por penalidades alternativas.

No entanto, mesmo com as mudanças referentes aos crimes virtuais, o Código Penal ainda é alvo de críticas por diversos doutrinadores e juristas. Acredita-se que a legislação não conseguiu acompanhar o crescente aumento de delitos digitais e a intensidade em que são praticados.

Ademais, as autoridades policiais enfrentam dificuldades nas investigações, diante da complexidade da zona virtual e do anonimato. Falta ainda recursos para o “desenrolar” das investigações, mesmo já existindo delegacias especializadas no combate ao cibercrime.

Acredita-se que o caminho mais fácil para a criação de uma legislação técnica, simples, adequada e eficaz frente a evolução tecnológica seria basear-se na nos preceitos da Convenção de Budapeste. Esse é inclusive o pensamento do Ministro Luiz Fux e dos doutrinadores Alessandro Gonçalves Barreto e Karina Kufa.

Neste sentido, a Convenção de Budapeste abrange estratégias e ferramentas, juntamente com outros países, sendo de extrema importância no combate ao cibercrime.

> Em vigor desde 2004, a Convenção de Budapeste de 2001 é um dos mais importantes instrumentos a lidar com aspectos penais substantivos, processuais e cooperativos no combate aos crimes cibernéticos e envolve mais de 60 países. Por seu caráter multilateral global e específico, ela reconhece o respeito às soberanias dos Estados signatários, preservação dos direitos e garantias fundamentais das partes e interesses das autoridades nacionais de aplicação da lei, em especial quanto ao objetivo de investigação e persecução de crimes praticados na internet e/ou com intermédio de ferramentas de internet e tecnologias digitais. (Conjur, 2021, online)

Sobre a Convenção, ainda complementa Fabricio Bertini:

> (...) Contempla estratégias conjuntas entre os países membros para a tipificação, combate e prevenção de crimes praticados pela internet, os delitos cibernéticos, e medidas de cooperação específicas para acesso a dados e informações digitais. (Conjur, 2021, online)

Dessa forma, o combate aos crimes virtuais ainda é um desafio para o Direito Brasileiro, e de acordo com inúmeros doutrinadores e juristas, esse problema poderia ser amenizado caso o governo se aliasse a referida Convenção, o que já foi sinalizado pelo Governo Federal e aprovado pela Câmara dos Deputados, uma vez que, as estratégias e medidas adotadas pelos países aliados já apresentaram um progresso significativo no combate ao cibercrime.

No entanto, esse é o assunto que deve ser analisado com mais cautela e com um estudo mais amplo e específico.

CONCLUSÃO

O presente trabalhou buscou analisar o surgimento da internet, bem como, as características e conceitos do cibercrime e do cibercriminoso, abordando, também, as tipicidades das principais condutas ilícitas praticadas no ambiente virtual. Teve como objetivo principal analisar as primeiras e principais medidas no combate ao cibercrime até as legislações atuais.

Diante das análises feitas ao longo de todo o trabalho, verifica-se extrema relevância do estudo quanto a temática dos crimes virtuais na atualidade. O cibercrime vem aumentando drasticamente, a medida em que a internet vai se expandindo e se tornando cada vez mais popular.

Os danos causados por essa modalidade delitiva são imensuráveis, provocando inúmeros impactos psicológicos, econômicos e financeiros. O combate exige um aperfeiçoamento tecnológico na esfera policial e judicial, o qual ainda se demonstra um desafio.

Verifica-se que a legislação brasileira não conseguiu acompanhar a rápida e intensa evolução dos crimes virtuais, sendo necessário uma legislação mais ampla, específica e eficaz para esse tema, necessitando de uma cooperação entre os Estados e entidades Internacionais para sua elaboração, como também para restar frutíferas as ações preventivas e repressivas, no âmbito judicial e policial.

Uma legislação baseada na Convenção de Budapeste pode trazer êxito no combate e prevenção ao cibercrime, no território brasileiro, mas este é um tema que carece de uma análise e estudo mais aprofundado, assunto para um trabalho póstero.

REFERÊNCIAS

AVORIO André e SPYER Juliano. **Para Entender a Internet versão revisada e ampliada**. 2015. p.189.

BRASIL. **Decreto de Lei nº 2.848, de 7 de dezembro de 1940. Código Penal**. Brasília, 1940. Disponível em: DEL2848 (planalto.gov.br). Acesso em: 17 abr. 2021.

BRASIL. **Lei 14.155 de 27 de maio de 2021**. Disponível em https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada.

CAPEZ, Fernando. **Curso de direito penal**: parte especial: arts. 121 a 212. São Paulo: Editora Saraiva, 2019. v. 2. 9788553609444. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553609444/. Acesso em: 10 out. 2020. Acesso restrito

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. Disponível em <http://www.nethistory.info/Resources/Internet-BR-Dissertacao-MestradoMSavio-v1.2.pdf>. Acesso em 15 de novembro de 2019.

CALDERON, Bárbara. **Deep & Dark Web**. Rio de Janeiro. Alta Books, 2017.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas reais**. Rio de Janeiro: Brasport, 2014.

CASTELLS, M. **A galáxia da Internet**: reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

CASTRO, Ana Lara; SYDOW, Spencer. **Stalking e Cyberstalking**: obsessão, internet, amedrontamento. Belo Horizonte: D' Plácido, 2017.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011. p.48.

_____. **Crimes digitais**. São Paulo: Saraiva, 2011.p.90

D'URSO, Luiz Augusto Filizzola. **Cibercrime**: perigo na internet. Publicado em 2017. Disponível em http://politica.estadao.com.br/blogs/faustomacedo/cibercrime-perigo-na-internet/>. Acesso em 25 de novembro de 2019.

MAIA, T. S. F. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro**. Universidade Federal do Ceará. Faculdade de Direito, Curso de Direito, Fortaleza, 2017. Disponível em:

http://www.repositorio.ufc.br/bitstream/riufc/31996/1/2017_tcc_tsfmaia.pdf Acesso em 18 set. 2021

MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 7 ed. São Paulo: Saraiva, 2011.

MILAGRE, José Antônio. **Lei Azeredo, AI-5 digital e a cultura do contra**. Jus Navigandi, Teresina, ano 14, n. 2216, 26 jul. 2009. Disponível em: https://jus.com.br/artigos/13211/lei-azeredo-ai-5-digital-e-a-cultura-do-contra . Acesso em: 15 set. 2021

MIRABETE, Júlio Fabrini. **Manual de Direito Penal**: Parte Especial, São Paulo: Atlas, 2006, p.29

NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo. BH Editora, 2008.

NUCCI, Guilherme de Souza. **Manual de direito penal**. Rio de Janeiro: Forense, 2014.

_____. Estatuto da Criança e do Adolescente Comentado. 3 ed. São Paulo: Revista dos Tribunais, 2016

PRADO, Luiz R. **Curso de Direito Penal brasileiro**: parte especial, 5 ed. São Paulo, Revista dos Tribunais, 2006, p.273

PRADO, Luiz Regis; CARVALHO, Érika Mendes de; CARVALHO, Gisele Mendes de. **Curso de direito penal brasileiro**. 13.ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2014

REIS, Wanderlei José dos. **Delitos cibernéticos**: implicações da Lei 12.737/12. Revista Jus Navigandi, Teresina, ano 19, n. 4007, 21 jun. 2014. Disponível em: https://jus.com.br/artigos/29647/delitos-ciberneticos-implicacoes-da-lei-12-737-12

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

SILVA, Gleyson V. dos S. **Aplicação da lei Maria da Penha em crimes virtuais**: a criminalização da pornografia de vingança. 2014. 30f. Trabalho de Conclusão de 62 Curso (Graduação em Direito- Universidade Estadual da Paraíba, Campina Grande, 2014.

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira**. (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017). Disponível em http://local.cnecsan.edu.br/revista/index.php/direito/article/view/468. Acesso em: 01 set. 2021

SOMADOSSI, Henrique. **O que muda com a Lei Geral de Proteção de Dados** (LGPD). Disponível em:

https://www.migalhas.com.br/dePeso/16,MI286235,31047/O+que+muda+com+a+Lei+Geral+de+Protec ao+de+Dados+LGPD.

VILHA, Anapatrícia Morales; Di Agustini, Carlos Alberto. **E-marketing para bens de consumo durável**. Rio de Janeiro. Editora FGV. 2002.

https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html. Acesso em 20 de novembro de 2019

https://primat2009.files.wordpress.com/2010/02/nocoes-basicas-de-internet.pdf Acesso em 20 de novembro d 2019

https://www12.senado.leg.br/noticias/materias/2021/04/05/lei-que-criminaliza-stalking-e-sancionada

https://analise.com/opiniao/lgpd-e-o-tratamento-de-dados-em-direito-penal

http://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd

https://www.conjur.com.br/2021-jul-05/polido-brasil-urgentemente-aderir-convencao-budapeste

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRÓ-REITORIA DE DESENVOLVIMENTO INSTITUCIONAL
Av. Universitária, 1069 | Setor Universitário
Caixa Postal 86 | CEP 74605-010
Goiânia | Goiás | Brasil
Fone: (62) 3946.3081 ou 3089 | Fax: (62) 3946.3080
www.pucgoias.edu.br | prodin@pucgoias.edu.br

RESOLUÇÃO n°038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante Mykaelly S. Lisboa Souza
do Curso de Direito, matrícula _____,
telefone: 62 99303-6558 e-mail mykaellysouza@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Cibercrimes e os reflexos no Direito Brasileiro.
_____,
gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 30 de novembro de 2021.

Assinatura do(s) autor(es): Mykaelly S. Souza
_____

Nome completo do autor: Mykaelly S. Lisboa Souza
_____

Assinatura do professor-orientador: _____

Nome completo do professor-orientador: _____