FACULDADE EVANGÉLICA DE RUBIATABA
CURSO DE DIREITO
MATHEUS RABELO BARROS

CRIMES CIBERNÉTICOS: UMA ANÁLISE DAS LEIS E DA SEGURANÇA BRASILEIRA FRENTE AO CIBERCRIME

RUBIATABA/GO
2021

MATHEUS RABELO BARROS

CRIMES CIBERNÉTICOS: UMA ANÁLISE DAS LEIS E DA SEGURANÇA BRASILEIRA FRENTE AO CIBERCRIME

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba, sob orientação da professora Especialista Lucivania Chaves Dias de Oliveira.

RUBIATABA/GO
2021

MATHEUS RABELO BARROS

CRIMES CIBERNÉTICOS: UMA ANÁLISE DAS LEIS E DA SEGURANÇA BRASILEIRA FRENTE AO CIBERCRIME

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba, sob orientação da professora Especialista Lucivania Chaves Dias de Oliveira.

MONOGRAFIA APROVADA PELA BANCA EXAMINADORA EM __ / ___ / ____

Especialista Lucivania Chaves Dias de Oliveira
Orientadora
Professor da Faculdade Evangélica de Rubiataba

Escreva a titulação e o nome completo do Examinador 1
Examinador
Professor da Faculdade Evangélica de Rubiataba

Escreva a titulação e o nome completo do Examinador 2
Examinador
Professor da Faculdade Evangélica de Rubiataba

Dedico este trabalho a minha mãe, que me apoia, me suporta e sempre acreditou em mim.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ser a luz que me guiou e me amparou durante toda minha vida.

Agradeço aos meus pais, por me apoiarem nesta escolha e estarem ao meu lado durante este momento tão especial.

Agradeço a meus amigos e companheiros pelas risadas, pela raiva que passamos juntos e pelos momentos divertidos que nunca serão esquecidos.

E, agradeço aos professores e a instituição que foram fundamentais para que eu pudesse alcançar o tão desejado curso de Direito.

RESUMO

Nesta pesquisa, foi estabelecido como problemática: diante da quantificação de crimes virtuais, atualmente existem leis suficientes para o seu combate legislativo? Dessa forma, se estabelece como objetivo geral verificar as vertentes penais protetivas das leis que combatem os crimes virtuais. Para isso, foi utilizado a metodologia de revisão de literatura qualitativa com método dedutivo. Assim, é possível realizar o entendimento penal e doutrinário sobre as principais características que remetem a evolução das leis frente aos crimes virtuais. Para isso, foram escolhidos artigos, sites, trabalhos acadêmicos, leis e doutrinas que remetem ao tema. Com exceção das leis, os periódicos coletados são entre os anos de 2000 a 2021. Como resultado, foi observado que 1 a cada 4 brasileiros já passou por algum golpe virtual, na qual é possível verificar que existem poucas leis para o setor e baixa penalização sobre os crimes virtuais. Isso foi perceptível baseado nos principais ataques de cibercrimes no Brasil, e na necessidade de atualização penal sobre a Lei Carolina Dieckmann e LGPD, como foi na tentativa pela aprovação da Lei 14.155/2021 buscou aumentar a quantidade da pena possível nos crimes informáticos, que era de apenas três meses a um ano, para quatro anos, podendo alcançar até oito anos de reclusão.

Palavras-chave: cibercrime; Direito; Lei Carolina Dieckmann; LGPD.

ABSTRACT

In this research, it was established as problematic: given the quantification of virtual crimes, are there currently enough laws for its legislative combat? In this way, the general objective is to verify the protective criminal aspects of the laws that combat virtual crimes. For this, a qualitative literature review methodology with a deductive method was used. Thus, it is possible to carry out a criminal and doctrinal understanding of the main characteristics that refer to the evolution of laws in relation to virtual crimes. For this, articles, websites, academic papers, laws and doctrines that refer to the theme were chosen. With the exception of the laws, the periodicals collected are between the years 2000 to 2021. As a result, it was observed that 1 in 4 Brazilians have already gone through some virtual scam, in which it is possible to verify that there are few laws for the sector and low penalty about cyber crimes. This was noticeable based on the main cybercrime attacks in Brazil, and the need for criminal update on the Carolina Dieckmann and LGPD Law, as in the attempt to pass Law 14.155/2021, it sought to increase the amount of punishment possible in computer crimes, which was from three months to one year, for four years, and may reach up to eigth years of imprisonment.

Keywords: cybercrime; Law; Law Carolina Dieckmann; LGPD.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

No século XXI, em meio aos diversos avanços tecnológicos, a internet se tornou fundamental na vida da população, com isso, as pessoas passaram a estar cada vez mais conectadas, aumentando consideravelmente devido ao isolamento causado pela pandemia do COVID-19. A internet se tornou uma necessidade, porém, mesmo diante das coisas boas que ela permite que sejam realizados, existem aqueles que sempre recorrem a métodos ilícitos buscando o ganho próprio sobre os outros.

Essas pessoas, chamadas de cibercriminosos, cuja nomenclatura também pode ser referenciada como cracker (quando possui conhecimento mais avançado sobre recursos informáticos), tendem a aplicar diversos crimes que não era tipificados na lei brasileira até o ano de 2012, os chamados cibercrimes, ou crimes virtuais.

Com o processo de tipificação dos crimes virtuais, o Direito pode especificar do que se tratam os termos informáticos e como os crimes podem ser adaptados para esse novo característica penal, pois, por mais que seja aplicado um roubo, injúria, dano moral, etc., o mesmo se configura como um crime do Código Penal, que não estava adaptado para a mesma prática em meios informáticos.

Dessa forma, baseado no pensamento de que o Direito possui apenas 8 anos de investimentos legislativos sobre leis focadas na internet, foi escolhido como problemática, diante da quantificação de crimes virtuais, atualmente existem leis suficientes para o seu combate legislativo?

O objetivo geral é de verificar as vertentes penais protetivas das leis que combatem os crimes virtuais. Quanto aos objetivos específicos, o primeiro visa destacar o cibercrime, suas características, perfil e principais ataques; descrever o histórico de atualização e criação das leis voltadas a informática durante os anos de 1996 até a atualidade; e avaliar a quantificação dos crimes virtuais durante a pandemia do COVID-19.

O interesse pelo tema adveio pelo grande aumento da utilização da tecnologia, consequentemente o grande aumento de crimes cibernéticos, havendo frente a sociedade que pouco entendia de como se prevenir ou agir diante desses casos. Alertar sobre a insegurança de empresas e pessoas físicas que utilizam o meio da informática para fins comerciais e financeiros. Analisar como o Brasil se sobressai diante das normas expostas pela legislação,

se estas são suficientes, e a importância de uma segurança especializada e inteligente para tratar esses tipos de crimes.

Assim, a escolha ocorreu porque os crimes virtuais são uma das principais ameaças do país, com as pessoas passando por situações de desinformação que possibilita a queda em golpes, principalmente no *phishing*, que se trata do golpe mais comum a ser aplicado. Dessa forma, agrega valor na literatura por especificas as principais proteções jurídicas destinadas a este tema, sendo fonte de informação para a população, citando também os crimes durante o período de pandemia do COVID-19.

Foi escolhido como metodologia a revisão de literatura qualitativa com método dedutivo. Assim, é possível realizar o entendimento penal e doutrinário sobre as principais características que remetem a evolução das leis frente aos crimes virtuais. Para isso, foram escolhidos artigos, sites, trabalhos acadêmicos, leis e doutrinas que remetem ao tema. Com exceção das leis, os periódicos coletados são entre os anos de 2000 a 2021, com o uso da base de dados do Google Acadêmico para a coleta dos dados.

Considera-se como hipótese a problemática realizada, a dificuldades legislativa em promulgar leis focadas no combate dos crimes cibernéticos na mesma velocidade em que eles representam perigo a sociedade, uma vez que existem poucas leis destinadas a nessa temática, enquanto a maioria dos crimes virtuais cometidos se relacionam com crimes do Código Penal de 1940.

Em relação a organização do trabalho, no capítulo dois foram descritos os principais entendimentos doutrinários que remetem os crimes virtuais, bem como o possível perfil dos envolvidos e os principais crimes cometidos. No capítulo três apresenta as leis que se relacionam com os crimes virtuais, apresentando as características básicas de crimes que estão dispostos no Código Penal, porém, apresentando também as leis destinadas totalmente na internet. E no capítulo quatro possui foco na apresentação da Lei Geral de Proteção de Dados de 2018, e na situação do cibercrime durante a pandemia do COVID-19, verificando padrões e leis criadas após 2018.

2. DOS CRIMES VIRTUAIS

Este capítulo apresenta as características sobre como os crimes virtuais são tipificados, assim, o leitor estará apto em entender como as leis tendem a ser criadas em relação a crimes que ainda não estão legislados, possibilitando a prevenção e o amparo sobre esse tipo de ataque. Então, o capítulo descreve o que é um crime virtual, qual o possível perfil dos criminosos que o praticam, quais os principais crimes cometidos no Brasil e sua relevância para que leis destinadas ao combate sejam desenvolvidas para proteção da população.

2.1 OS CRIMES VIRTUAIS NUM CONTEXTO GERAL

O crime cibernético, também conhecido crime virtual, refere-se as ações ilegais cometidas por meio da tecnologia ou por meio recursos informáticos. Trata-se de um comportamento ilegal onde o autor recorre a um computador, celular, ou qualquer outro aparelho de informática ou que pode ser conectado à internet, justamente pela aplicação ser realizada em ambiente virtual (JORGE; MILAGRE, 2016).

Na doutrina, os crimes cibernéticos são divididos em crimes próprios e crimes impróprios. A qualificação como crime próprio ocorre quando as ações do autor do crime visam prejudicar um sistema ou infringir dados, como por exemplo, invasão de sistemas para destruir ou impedir o funcionamento de um servidor de um site ou de uma empresa. A qualificação como crimes impróprios ocorre quando se trata de um crime que também pode ser realizado fora da internet, como por exemplo o estelionato (AZEVEDO; CARDOSO, 2021).

Nos crimes impróprios, destacam-se como mais comum na internet o discurso de ódio. Neste caso, por mais que a liberdade de expressão seja um direito garantido por lei, ela não pode ultrapassar os limites dos direitos de terceiros e se opor à imagem, privacidade, honra, intimidade, etc. porque pode se figurar em crimes contra a honra, assédio ou difamação (AZEVEDO; CARDOSO, 2021).

Em relação ao perfil do autor, quando se trata de um crime praticado na internet, as pessoas tendem a imaginar que ele seja realizado por alguém com habilidades especiais no computador, como se fosse um gênio que usa sua sabedoria para fazer o mal, mas esse

pensamento é equivocado. Atualmente, qualquer pessoa com o mínimo de conhecimento em informática pode cometer crimes virtuais.

Diante dessa situação, fica claro que identificar criminosos digitais não é fácil, porque ele não possui as mesmas características dos criminosos tradicionais, que detêm um perfil observado na sociedade em relação a uso de tatuagens, cor da pele e classe. Além disso, por estarem em anonimato, principal benefício que o uso da internet permite, se tornam uma ameaça invisível que pode ser representado desde um jovem de 16 anos, até um idoso de 80 que não transparecem qualquer sinal de perigo (BRITO, 2013).

No entanto, mesmo diante da dificuldade de identificar os autores dos crimes virtuais, é padrão em seu perfil que precisam de conhecimento de tecnologia da informação, eletrônica e redes de computadores. Quando a pessoa realmente possui conhecimento mais elevado em informática, tendem a ser chamados de hackers ou crackers, porém, em crimes virtuais, são os crackers que realizam ataques visando ganho próprio.

Enquanto isso, o termo hacker não significa que o sujeito seja um criminoso, muitos dos quais usam seus conhecimentos e habilidades para bons propósitos, por exemplo, podem se tornar a força de trabalho de empresas relacionadas ao uso da Internet e desenvolver sistemas informáticos seguros.

Assim, parte-se do entendimento de que criminosos virtuais são aqueles que recorrem ao uso de equipamentos informáticos para a prática de crimes, crimes esses que são comuns no Brasil e que demandam inúmeros tipos de golpes que atingem a população, e se tornam em característica geral a ser observada pelo Direito para atualização das leis destes delitos.

2.3 OS CRIMES VIRTUAIS NO BRASIL

Para esclarecer a importância deste tema, foram descritos quais os principais crimes virtuais com maior incidência no Brasil. Os dados foram divulgados pelo DFNDR Lab (Figura 1) no terceiro trimestre de 2017, e com base nos dados coletados, mais de 21 milhões de ataques de segurança foram identificados, principalmente sendo ocorridos por *smartphones*.

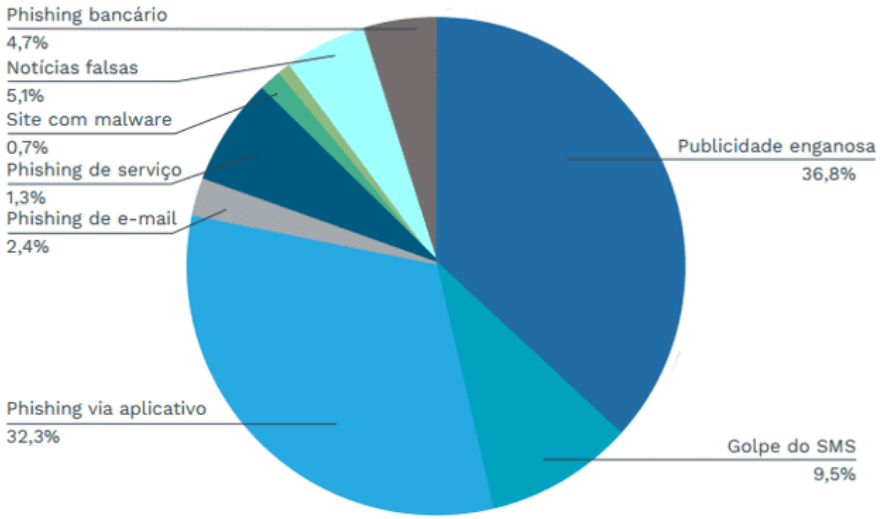

Figura 1 – Dados de ataques cibernéticos durante o ano de 2017
Fonte: Silva e Vieira (2021).

Como observado na imagem, um nome aparece diversas vezes no gráfico, sendo aquele que mais afeta o mundo, e, o mais sofrido pelos brasileiros, são os chamados ataques de *phishing*. Por se tratar do ataque mais comum, é possível atualizar a legislação combatendo tais crimes em particular, e mostrar que o direito penal precisa sempre estudar os crimes que estão sendo perpetrados pela Internet no mundo para que a proteção de usuários mais rápida e eficaz (KAPERSKY, 2018).

O termo *phishing* vem do termo *fishing*, que significa pescar em inglês, ou seja, os criminosos recorrem a mensagens falsas que são compartilhadas entre as pessoas, servindo como isca. Assim, aguardam pacientemente até que alguém fisgue e passe suas informações pessoais. As informações são passadas porque geralmente são utilizados sites clonados de empresas reais, então, a pessoa sem perceber, ao tentar entrar com seu acesso, acaba fornecendo sua senha sem perceber, que pode ser utilizada pelos criminosos que a registram. Se trata, então, de uma fraude eletrônica e um ataque sério, pois quem comete a fraude pode obter da vítima as senhas, dados financeiros, cartões de crédito e outras informações (MORGENSTERN; TISSOT, 2015).

Esse golpe ainda pode ser dividido em métodos, onde o mais comum é chamado *scam*. Ele consiste no envio de e-mails fraudulentos de uma empresa conhecida do público, tentando persuadir a vítima que se tratam de informações verdadeiras, levando a uma página clonada que, geralmente, solicita que as informações pessoais sejam colocadas, na maioria dos casos, informações confidenciais como um número de conta, senha da conta pessoal, senha do cartão, etc. (JORGE, 2007).

Além *scam*, também podem recorrer as outras fontes, conforme a Figura 1 apresentou, sendo o envio via aplicativos o segundo maior. Como os aplicativos como o WhatsApp se tornaram algo cultural de uso, principalmente na interação em grupos, muitos casos de compartilhamento de links fraudulentos podem ser recebidos expondo as pessoas ao perigo (PEREIRA; MARTINS, 2014).

Esse tipo de ataque aumentou muito o número de vítimas em todo o mundo. Ameaças, desvio de fundos públicos, extorsão, roubo de identidade, perseguição e clonagem de cartão são apenas algumas das ameaças representadas por esses ataques hoje. Estima-se que, nos últimos anos, esse tipo de mídia tenha se tornado um dos favoritos para a mineração de informações e a taxa de uso dos profissionais tenha aumentado em mais de 60% (CORTELA, 2013).

Além de usar mensagens aleatórias para esperar que alguém caia neste golpe, os criminosos que implementam *phishing* também combinam técnicas de engenharia social e manipulação de informações e clonagem de páginas para enganar vários perfis de usuários. Permite manipulá-lo indiretamente simulando um site oficial, tentando roubar os dados pessoais da vítima pela sua própria ingenuidade. Portanto, o uso de nomes de bancos, lojas e empresas famosas é a base da prática deste ataque, criando réplicas quase perfeitas para obscurecer qualquer possibilidade de identificação. (LAS-CASAS et al., 2016).

Por exemplo, quando um conhecido ou parente compartilha uma mensagem no grupo falando sobre uma promoção de uma loja, sendo necessário apenas realizar o acesso para participar. A pessoa, por observar que foi enviada por conhecido, acaba confiando no link enviado, porém, ambos podem ter se tornado vítimas do criminoso, que recebe o acesso com os dados de senhas dessas pessoas.

Isso ocorre principalmente na versão mobile, como na Figura 2, numa tentativa de golpe utilizando a página do Banco do Brasil, o site direciona para que a pessoa coloque seus dados, que pensa que está atualizando sua conta. Como nesses caso o golpe pode ser enviado por aplicativos de mensagens, é mais fácil para os criminosos enganar as vítimas, que fazem menos checagens pelo celular, em comparação ao que seria o site via computador.

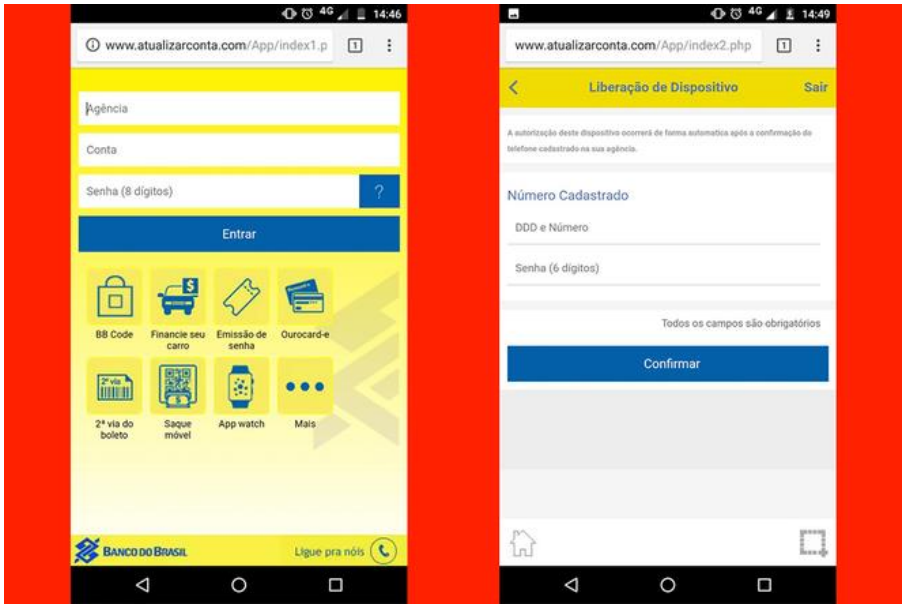

Figura 2 – Site clonado do aplicativo do Banco do Brasil
Fonte: Agrela (2017).

Porém, conforme recomendações de segurança da internet, mesmo considerando a semelhança, é possível identificar quando uma página é fraudulenta. O primeiro passo é observar o site, conforma a Figura 2, observa-se no rodapé da figura da esquerda que aparece a frase "ligue para nóis". Se este fosse o site oficial do Banco do Brasil, não haveriam erros gramaticais no texto, o que deve ser suficiente para que o usuário não precise preencher os dados solicitados pelo menos antes de entrar em contato com o banco.

Outro ponto fundamental a ser observado remete ao site, na Figura 2, o nome do site está “www.atualizarconta.com”, sendo que o site oficial do Banco do Brasil é o “www.bb.com.br”. Logo, um site que não apresenta o nome correto do site da empresa possui altíssima porcentagem de ser falso, e deve ser observado pelo usuário antes de digitar qualquer informação na página.

Em pesquisa realizada em 2018 pelo antivírus Kapersky, o Brasil ocupa a primeira posição no mundo em ataques de *phishing*. Em 2017, quando descobriu que quase 30% dos internautas do país haviam sofrido pelo menos uma tentativa de golpe, a posição foi assegurada. Mesmo o índice caindo para 23% em 2018, não foi o suficiente para tirar o Brasil dessa posição, confirmando que o *phishing* de WhatsApp é atualmente a prática mais comum, conforme mostra a Figura 3 (KAPERSKY, 2018).

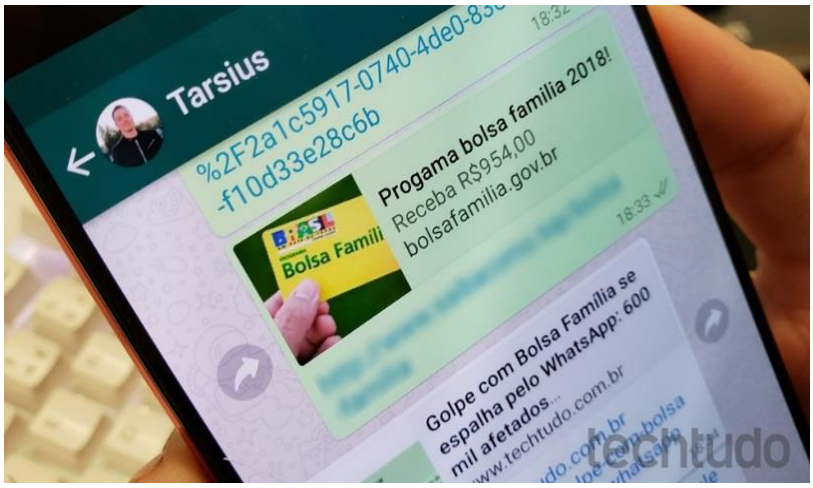

Figura 3 – *Phishing* usando o Programa Bolsa Família como estratégia de golpe pelo WhatsApp
Fonte: TechTudo (2018).

Mesmo que a identificação dos sites fraudulentos possa ser realizada apenas observando com atenção os sites acessados, outro motivo que torna esses ataques tão propícios ao sucesso remete ao erro humano e a falta de preocupação aos possíveis problemas e vulnerabilidades do sistema. Como o *phishing* consiste num golpe fácil e barato para ser aplicado, as pessoas não imaginam que o site acessado se trata de uma página clonada que visa a coleta de dados pessoais para serem usados em golpes e clonagem de cartão (KAPERSKY, 2018).

À medida que a tecnologia se torna cada vez mais segura e eficiente para os humanos, essa prática se torna mais comum porque não necessita que o próprio criminoso invada o celular da vítima, pelo contrário, é a vítima que acaba passando seus dados sem perceber. Essa relação entre a prática do crime e a estratégia utilizada parece difícil de entender, porém, trata-se de uma estratégia de ponte para um crime maior, seja roubo de informações pessoais, fotos privadas, clonagem de cartões, informações confidenciais da empresa, etc. (SILVA et al., 2021).

Portanto, ao compreender os principais conceitos relacionados ao cibercrime e os principais crimes cometidos no Brasil e no mundo, agora é possível mostrar o que os indivíduos podem fazer para se protegerem, descrevendo no próximo capítulo quais as leis focadas para Internet já existem no Brasil.

3 DAS LEIS ENTRE 1996 A 2017 VOLTADAS PARA A PROTEÇÃO CONTRA O CIBERCRIME

Neste capítulo, foram descritas as principais contravenções penais que remetem a prática de cibercrimes. No período anterior a 2012, não havia sido criada nenhuma lei que fosse exclusiva para crimes virtuais, na qual os crimes se relacionavam com aqueles impostos no Código Penal.

A prática de atos antiéticos e ilegais utilizando-se meios digitais não o isenta da caracterização de crime. A sensação de anonimato não passa de ilusão, esse tipo de conduta é classificado no Ordenamento Jurídico como crime e possui sanções penais previstas em lei. Dessa forma, no Código Penal é possível observar inúmeros crimes que estão relacionados aos crimes impróprios do cibercrime (SCHAU, 2019).

Pode-se destacar calúnia (art. 138), difamação (art. 139), injuria (art. 140), ameaça (art. 147), divulgação de segredo (art. 153), invasão de dispositivo informático (art. 154-A), furto (art. 155), dentre diversos outros crimes (BRASIL, 1940). Ou seja, percebe-se que inicialmente os crimes virtuais são tratados na tipificação dos crimes penais, uma vez que não existia lei que especificasse e vincula-se os crimes ao serem cometidos através de recursos informáticos.

Porém, mesmo diante dessas pequenas atualizações que a lei foi adaptando ao longo do seu histórico, duas leis se destacam durante esse período de tempo, sendo consideradas marcos na atualização do Direito frente ao combate à crimes virtuais, sendo as chamadas lei Caroline Dieckmann e Marco Civil da Internet.

3.1 LEI CAROLINE DIECKMANN (LEI N. 12.737/12)

É interessante observar que as leis que surgiram a partir de 2012, que versam sobre a temática de cibercrime, foram resultado de pressão da mídia sobre o poder legislativo. Nesse cenário, cita-se as Leis nº 12.735/12 e 12.737/12, sendo que a primeira trouxe alteração legislativa do Código Penal, do Código Penal Militar e da Lei de Preconceito, tipificando os crimes realizados na internet, e a segunda dispõe a respeito da tipificação dos crimes informáticos, além de alterar o Código Penal (CRUZ; RODRIGUES, 2018).

A Lei Ordinária 12.735/12 se tratou da transformação do projeto de lei 84/99, e foi nomeado de “Lei Azeredo”, trazendo as primeiras disposições sobre crimes, penas e outras providências cometidos por meio virtual, que alterou somente o inciso II do parágrafo 3° do art. 20 da Lei n° 7.716/89 (Lei do Crime Racial), para proibir conteúdos discriminatórios na rádio, televisão ou internet, e por qualquer forma possível, a pedido do juiz, e para combater as atividades criminosas praticadas através da Internet ou de sistemas informáticos, determinou também que a Polícia Judiciária tenha o responsabilidade de estabelecer delegacias especiais de polícia (BRASIL, 2012a).

Porém, essa lei ainda não atribuía a proteção aos objetos jurídicos sobre a liberdade pessoal de usuários de equipamentos de informática, devido a essa "lacuna", ocorreu o escândalo midiático da divulgação de fotos íntimas da atriz Carolina Dieckmann, tornando presente o problema em questão, e levando a sanções urgentes contra a referida do caso, sendo criada a Lei nº 12.737/2012.

Caetano (2015), destaca como a pressão da mídia contribuiu consideravelmente, uma vez que o caso ganhou repercussão nacional, dessa forma, a lei permitiu a tipificação criminal de delitos informáticos, alterando o Código Penal ao acrescentar dois artigos, o art. 154-A e 154-B.

> 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 (BRASIL, 2012b).

No artigo 154-B, conforme os crimes tipificados no artigo acima, é praticado somente por intermédio de órgão, a menos que o crime seja cometido contra órgão da administração pública direta ou indireta de qualquer poder da União, seja Estadual, do Distrito Federal ou Municipal (BRASIL, 2012b).

Mesmo diante das inovações criminais mencionadas, o Diploma Normativo tem recebido algumas críticas, pois embora seja um crime informático típico, não pode prever todos os crimes possíveis e também é tecnicamente frágil. Porém, como antes dessa inovação no Direito Penal, não existiam dispositivos legais no ordenamento jurídico que tipificassem os crimes acima divulgados e impunham os criminosos, se tornou a base para julgar os crimes envolvendo recursos informáticos (NASCIMENTO, 2019).

Portanto, as ações realizadas atrás de uma tela de computador não podem ser isentas de responsabilidade civil ou criminal. Se alguém não cumprir a lei e cometer o crime

de colocar a honra ou a condição de alguém em risco, mesmo recorrendo a meios indiretos para aplicação do crime, como a internet permite, o agressor ainda pode ser responsabilizado pelos seus atos (SANTOS, 2020).

Além da alteração descrita anteriormente, a Lei n° 12.737/2012, também alterou o artigo 266 e 298 do Código Penal, incluindo no crime de interrupção de serviço, os serviços telemáticos ou de informação de utilidade pública; e nos crimes de falsificação de documentos foi incluído a falsificação de cartões de crédito/débito (BRASIL, 2012b).

Um dos principais problemas também destacados desta lei remete a, que ao ser considerado culpado, pode levar entre 3 meses a 1 ano de reclusão e multa. Situação que levou a inúmeras críticas, pois ao passar pouco tempo de reclusão, não torna a lei totalmente preventiva de que os responsáveis pela prática do crime não vão continuar cometendo-os, ressaltando na alta taxa de golpes sofridos pelos brasileiros anualmente.

3.2 MARCO CIVIL DA INTERNET (LEI N. 12.965/14)

A Lei n.º 12.965/14 foi submetida à Assembleia Nacional em 2011 pelo chefe do Poder Executivo, transformando-a na Lei n.º 2.126/2011. Assim, foi publicado em 23 de abril de 2014. Seu principal objetivo é estabelecer princípios, garantias e obrigações para o uso da Internet no Brasil.

A Lei n° 12.965/14, popularmente conhecida como Marco Civil da Internet certifica um procedimento mais ágil para a remoção de mídias íntimas que foram expostas no ambiente virtual, e a Lei nº 13.718/2018, que somou um novo delito no art. 218-C, do Código Penal:

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave. (BRASIL, 2018).

Devido a crescente funcionalidade que a internet foi adquirindo e seu acesso foi se tornando essencial à vida das pessoas, a lei foi criada com intuito de regularizar essas utilizações e eliminar a ideia de que a internet é uma “terra sem lei”. Nascimento (2019) explica que o Marco Civil da Internet ficou popularmente conhecido como a Constituição da

Internet Brasileira e é composto de 10 (dez) princípios elaborados pelo Comitê Gestor da Internet brasileira.

Os 10 (dez) princípios previstos na Lei do Marco Civil são

> [...] liberdade, privacidade e direitos humanos; governança democrática e colaborativa; universalidade; diversidade; inovação; neutralidade da rede; inimputabilidade da rede; funcionalidade, segurança e estabilidade; padronização e interoperabilidade; e ambiente legal e regulatório.

Seguindo esses princípios, a lei também permitiu a tipificação de diversos termos informáticos, como registro de conexão, sendo o conjunto de dados sobre a hora inicial e final do acesso à internet. E os registros de acesso a aplicações de internet, constando os dados de acessos realizados, sendo descrito a hora e a data, a partir de determinada aplicação (BRASIL, 2014).

O registro da conexão é mantido pelo provedor de acesso, composto pelas pessoas jurídicas que prestam serviços de acesso à Internet em banda larga. O registro da conexão é mantido pelo provedor de acesso, que é composto pelas pessoas jurídicas que prestam serviços de acesso à Internet em banda larga (LIMA, 2016).

Em Recurso de *Habeas Corpus* 117.680 do Pará, em 2020, o Superior Tribunal de Justiça entendeu que o tempo de registro se configura no fluxo de comunicações que relatam os acessos e as funcionalidades acessadas pelo terminal com internet, evitando que o autor do ato testemunhe sobre o período de tempo de uso e acesso, sendo característica estatística que pode ser utilizada nos julgados (BRASIL, 2020).

Mesmo assim, ainda demanda forte dificuldade na punição de criminosos virtuais, principalmente porque é um desafio investigativo encontrar quem se esconde no anonimato. Além da aplicabilidade efetiva das leis existentes, outras leis ainda precisam ser formuladas para efetivar a condição atual de combate (JESUS; MILAGRE, 2016).

Outra crítica apontada refere-se ao caráter simbólico que o Marco Civil da Internet representa, porque muito de seus artigos relatam condições jurídicas constitucionais, logo, se torna passível de entendimento legislativo para que suas prerrogativas sejam exercidas (RODRIGUES, 2014).

Além disso, o artigo 19 da lei também estipula outros requisitos para a responsabilidade penal do cumprimento, na qual um mandato só é permitido mediante descrição clara e completa sobre o que se deseja buscar e quais os principais serviços informáticos estão sendo utilizados (BRASIL, 2014).

É por isso que no fim, uma das mais importantes atividades a serem realizadas cabe na orientação dos cidadãos, principalmente crianças e adolescentes usuários de redes digitais sobre seus direitos de dados e, principalmente, da responsabilidade dos prestadores de serviços digitais que são a base para que as instituições judiciárias enfrentem as infrações e os riscos da sociedade da informação que podem estar sujeitos a choques tecnológicos (JESUS; MILAGRE, 2016).

3.2 CYBERBULLYING (LEI N. 13.185/15)

A tecnologia se tornou inevitável na vida de todos e trouxe inúmeros benefícios para cotidiano, tornando impossível imaginar um mundo sem a Internet. No entanto, apesar da grande revolução no campo das comunicações, algumas pessoas ainda encontram oportunidades de cometer crimes cibernéticos (GONÇALVES; OLIVEIRA, 2020).

Infelizmente, os crimes que visam golpes nas pessoas não são os únicos preocupantes, visando afetar a pessoa indiretamente com inúmeros casos de discurso de ódio, ameaça, e outras situações, o chamado *cyberbullying*. Para entendê-lo melhor, é necessário saber o que é *bullying*. A palavra *bullying* vem do inglês, na tradução livre do português significa valentão, brigão, etc. (BRITO, 2013).

Na Lei nº 13.185/15, sancionada em 6 de novembro de 2015, o *bullying* é definido como a atividade sistêmica realizada por uma ou mais pessoa contra alguém, recorrendo a violência física ou psicológica, buscando a intimidação, constrangimento, dor e sofrimento. Neste crime também pode existir uma relação hierárquica entre os envolvidos (BRASIL, 2015).

Embora seja mais comum nas escolas, é indiscutível se trata de um crime que pode aparecer em todas as relações que envolvem determinados níveis, como as relações de trabalho entre chefe e funcionários ou entre professores e alunos, podendo ocorrer em qualquer idade, horário, classe social, ou localização (RODER; SILVA, 2018).

Em 2018, o Brasil se tornou o segundo país do mundo com mais casos de *cyberbullying*. Aumentando a preocupação para o combate deste crime. Dessa forma, nos casos julgados de *cyberbullying*, o mesmo pode se relacionar com os artigos do Código Penal, ou seja, o julgado pode ser enquadrado em crimes de calúnia, difamação, injúria, falsa identidade e racismo (CONTE, 2010).

Dessa forma, apesar da promulgação das leis supramencionadas, os demais cibercrimes continuam a serem julgados com base nos efeitos dos danos causados. Cruz e Rodrigues (2018) apontam que a maior dificuldade encontrada nos cibercrimes reside nas questões técnica de como chegar no infrator e a quem pertence a competência de julgamento, e não somente na ausência de lei que classifique e puna os crimes virtuais.

Assim, pode-se verificar que o Direito possui diversas atualizações frente as tecnologias desde 1996, destacando os anos de 2012 e 2014 como os principais para a área de informática. Com isso, o capítulo seguinte visa descrever as leis impostas entre 2018 até 2021 para esta área, principalmente na Lei Geral de Proteção de Dados Pessoais (LGPD), e o combate aos crimes virtuais durante o período de pandemia do COVID-19 que se iniciou em dezembro de 2019 na China.

4 O COMBATE AO CIBERCRIME ENTRE 2018 À ATUALIDADE

Neste capítulo foi apresentado as principais leis e características do cibercrime de 2018 até 2021, ano de entrega deste trabalho. Em três anos, existiram três principais condições que remetem ao cibercrime e merecem destaque, sendo o primeiro a Lei Geral de Proteção de Dados Pessoais, que visou tipificar e melhorar o controle de acesso e de armazenamento de dados, melhorando questões não avaliadas no Marco Civil da Internet.

A questão da pandemia do COVID-19 e como os cibercrimes estão sendo autuados, sendo importante para verificar se neste momento de isolamento, onde as pessoas necessitaram estar mais conectadas na internet, se os casos reduziram ou aumentaram, o mesmo destacando em relação a lei.

E, por último, a lei que foi sancionada em 2021, buscando solucionar um dos principais problemas observados ao longo desta temática, sobre a quantidade da pena dos culpados, de forma que melhore o processo de combate ao cibercrime, principalmente no decorrer da pandemia do COVID-19.

4.1 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD (LEI N. 13.709/18)

Foi sancionada a lei nº 13.709 em 14 de agosto de 2018, que ficou conhecida como Lei Geral de Proteção de Dados (LGPD), baseada nas normas europeias de proteção de dados. De destaque, essa lei buscou a autodeterminação informativa para fundamentar as principais questões sobre a proteção dos dados (art. 2º, inciso II). Com ela, ocorreram mudanças em relação ao entendimento do acesso às informações em banco de dados privados (LARA, 2019).

> Para compreender a LGPD, é preciso analisar os seus princípios e bases legais. Por conseguinte, quando trata de dados pessoais a lei tem como base: a finalidade de tratá-los de forma específica, legítima, explícita e informada; a adequação à coerência do uso da informação solicitada; a necessidade do uso, limitado de dados essenciais para a finalidade apresentada; o livre acesso de consulta da pessoa titular; a qualidade dos dados, garantia da veracidade e atualidade deles; a transparência, ao titular, do uso dos dados; a segurança para impedir a invasão, destruição, perda ou difusão destes; a prevenção, a fim de evitar danos em razão do tratamento; a não discriminação, ou seja, não é permitido descriminar ou promover abusos conta os seus titulares; a responsabilidade e prestação de contas das empresas para comprovar que estão agindo de acordo com a lei (BRASIL, 2018).

Com isso, a LGPD busca a garantia da proteção de dados dos brasileiros, e para este fim ela determina em quais tipos de dados aplica-se. O primeiro são os dados pessoais, aqueles que dispõem informações que permitem identificar um indivíduo de forma direta ou indireta, sendo assim, o CPF e telefone são classificados como tais (BRASIL, 2018).

O segundo são os dados pessoais sensíveis, que complementam o anterior, contudo carece de maior atenção em razão de tratarem de crianças e adolescente e/ou possuírem dados sobre a origem racial ou étnica, referente à saúde ou à vida sexual, dado genético ou biomédico vinculados a uma pessoa natural, convicção religiosa, opinião política e filiação a sindicato ou organizações de cunho religioso, filosófico ou político (BRASIL, 2018).

A nova legislação se aplica para o tratamento de dados pessoais coletados no território nacional, que tenham como finalidade a oferta de bens e serviços para indivíduos situados no Brasil. Todavia, esta não é destinada para o uso pessoal, não comercial, fins jornalísticos, artísticos ou acadêmicos, segurança pública e dados provenientes ou destinados a outros países (BRASIL, 2018).

Com isso, ela permite que o princípio da adequação esteja intimamente relacionado ao princípio da finalidade, uma vez que ocorre a compatibilidade do processamento de dados apenas mediante o consentimento do titular dos dados. É a exatidão e adequação do conteúdo notificado ao titular no momento da coleta de dados e o conteúdo efetivamente utilizado.

Com isso, depois de sancionada, foi possível perceber que inúmeras empresas atualizadas suas políticas de privacidade de várias, em especial o Facebook, que passou a ter uma transparência muito maior do uso dos dados pessoais de seus usuários. Neste caso é mais perceptível, principalmente devido aos inúmeros casos de vazamentos de dados que a empresa foi processada, fazendo com que ela criasse uma página especifica para “Verificação de Privacidade” com as opções: “Quem pode ver o que você compartilha”; “Como manter sua conta segura”; “Como encontrar você no Facebook”; “Suas configurações de dados no Facebook”; “Suas preferências de anúncios no Facebook”. Logo, possibilita que o usuário adquira maior segurança e privacidade, visto que possui o poder de decidir quais dados e com quem deseja compartilhá-los (BRASIL, 2018).

Esse tipo de lei também se configurou na conduta da propaganda, porque os dados podem não só identificar o dono, mas também toda a sua vida, seus hábitos, seus gostos e desgostos, e o uso dos dados se tornou amplamente utilizado para converter vendas, porque

dessa forma, os sites coletavam os dados pessoais e repassavam para lojas de acordo com o perfil do usuário, que passava a ver anúncios online correspondem aos seus gostos.

No panorama do ordenamento jurídico brasileiro, o reconhecimento de que a proteção de dados é um direito autônomo e básico não decorre de termos claros e literais, mas da consideração dos riscos que o processamento automatizado traz à proteção da personalidade. A Constituição garante a igualdade substantiva, a liberdade e a dignidade das pessoas, bem como a proteção da intimidade e da privacidade.

Isso produziu uma mudança abrangente na cultura atual, que pode ser exemplificada nos termos de uso de qualquer site com "Eu li e concordo". Ao longo dos anos, poucas pessoas realmente leem esses termos, e algumas empresas utilizavam desta brecha para vincular os dados de usuários em outros processos, com o consentimento subjetivo do usuário que aceitou o termo sem saber do que se tratava de fato.

Pode-se citar a Ação Civil Pública Cível n. 0733785-39.2020.8.07.0001 de 2020, julgado pela 17ª Vara Cível de Brasília, na qual uma empresa de comércio eletrônico foi processada por uso indevido de dados pessoais. O autor provou na ação que o comércio eletrônico é um intermediário para a comercialização em larga escala de dados pessoais. Além disso, um vendedor realizava atividades por meio de um portal na Internet, fornecia cadastros e bases de dados gerais, sendo o réu o beneficiário do pagamento (BRASIL, 2020).

Assim, o juiz realizou o entendimento de que as provas dos autos revelaram que existia comércio dos dados pelo réu, ferindo o art. 5º, I, da LGPD. Referindo-se também o art. 44 da lei:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I – o modo pelo qual é realizado;
> II – o resultado e os riscos que razoavelmente dele se esperam;
> III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (BRASIL, 2020).

Está prática fere o princípio constitucional da inviolabilidade do sigilo de dados, insculpido no artigo 5º, XII, da Constituição Federal, o juiz concedeu a tutela de urgência proposta na denúncia e ordenou ao réu da empresa de comércio eletrônico que não fornecesse dados pessoais de forma gratuita ou onerosa, sendo multado em 2.000 reais por cada infração (BRASIL, 2020).

Ou seja, essa lei já está em aplicação na jurisprudência, possibilitando o amparo da população brasileira frente aos casos de uso irregular dos dados pessoais. Mesmo assim,

observa-se que este problema está longe de acabar, principalmente quando observado a situação que o país se encontra frente aos cibercrimes durante a pandemia do COVID-19.

4.2 DO COMBATE AO CIBERCRIME DURANTE A PANDEMIA

A pandemia do COVID-19 levou as pessoas a se tornarem mais solitários devido ao isolamento social, porém, se tornaram mais conectados na internet. Em casa, as pessoas estão cada vez mais habituadas a participar de redes sociais, vídeo-chamadas, grupos da família, encontros virtuais, dentre outros habilidades obtidas pelo uso da tecnologia (BOTTINI, 2020)

O isolamento social e maior uso dos recursos informáticos teve um impacto no campo do crime. Os crimes que exigem que as vítimas sejam fisicamente vulneráveis diminuíram. Em março de 2020, São Paulo viu uma redução de 13.917 furtos, representando uma queda de 30% em relação ao total de crimes do mesmo período do ano passado. Da mesma forma, o tráfico de drogas diminuiu devido à falta de instalações comerciais reais e à dificuldade de obtenção de matéria-prima para a fabricação de compostos ilegais. Por outro lado, o número de ataques a mulheres aumentou 44,9%, e a morte de mulheres aumentou 46,2% (BOTTINI, 2020).

Em relação aos crimes virtuais, com o isolamento, as pessoas buscam realizar a maioria de suas atividades online, seja compras, trabalho, envio de dinheiro, etc. A insegurança e a falta de compreensão desses mecanismos de aquisição e transferência virtual de mercadorias tornam as pessoas passiveis de diversos golpes, como páginas falsas de bancos e lojas na Internet, muitas das quais veiculam anúncios promocionais imperdíveis (BOTTINI, 2020).

A TransUnion, empresa global destinada a análise de dados, confirma novamente que o crime virtual mais comum no Brasil durante a pandemia de COVID-19, foi o *phishing*, que é o uso de isca para roubar dados, como recompensas eletrônicas ou cobranças falsas (SAKATE, 2020).

Ao mesmo tempo, Satake (2020), em análise ao estudo da TransUnion, percebeu que um em cada quatro brasileiro já foi vitima de crimes envolvendo cartões de crédito. Em entrevista realizada com a população sobre os possíveis crimes que cada pessoa já pode ter sofrido, a Tabela 1 pode perceber os seguintes dados.

Tabela 1 – Porcentagem de casos envolvendo cibercrime, com cada pessoa relatando mais de um caso

Tipo de crime	Porcentagem
Phishing (roubo de dados)	27%
Golpe de falsos vendedores varejo online	21%
Fraude envolvendo caridade de arrecadação de fundou	19%
Golpe em desempregados	18%
Vacina de COVID-19, curas e testes	15%
Fraude em seguros	15%
Fraude de envio de produtos	14%
Roubo de identidade	14%
Cartão de crédito roubado ou cobrança fraudulenta	13%
Golpe do "benefício do governo"	12%

Fonte: Sakate (2020, p. 1).

Novamente o *phishing* aparece na liderança, o que significa que mediante a pandemia do COVID-19, esse tipo de golpe se mantém com alta frequência na população, podendo ressaltar também alguns golpes específicos ao período, como golpes envolvendo a vacina do COVID-19 e os golpes do "benefício do governo" (SAKATE, 2020).

Infelizmente, devido a quantidade de noticias falsas espelhadas nas redes sociais e aplicativos, estima-se que mais de 11 milhões de acessos e compartilhamentos foram realizados sobre golpes informáticos, observando a gravidade deste problema no país, que também se intensifica com o compartilhamento de notícias falsas (*Fake News*) (BOTTINI, 2020).

Porém, mesmo diante dessa condição, em 2021, foi aprovada mais uma lei com objetivo de aumentar a segurança frente aos cibercrimes, demonstrando que mesmo diante das dificuldades que o país enfrenta, o Direito busca adequações conforme a possibilidade legislativa.

4.3 LEI N. 14.155, DE 27 DE MAIO DE 2021

A primeira aprovação desta lei ocorreu no dia 15 de abril de 2021 na qual foram realizadas alterações no projeto de lei 4554/2020, que prevê alterações no Código Penal, no artigo 155 em relação a furto e fraudes eletrônicas. A nova alteração previu penas maiores para este tipo de crime, aumentando de quatro a oito anos, em vez da anterior era no máximo quatro anos de reclusão (AZEVEDO; CARDOSO, 2021).

No dia 28 de maio de 2021, foi sancionada a Lei 14.155, de 2021, tornando mais duras as penas sofridas nos crimes virtuais como fraude, furto e estelionato praticados com o uso de dispositivos eletrônicos como celulares, computadores e tablets. Esse foi um passo fundamental, uma vez que um dos principais problemas da proteção contra cibercrimes nas leis remete a quantidade da pena para o infrator (BRASIL, 2021).

De acordo com a nova redação do código, o crime de invasão de equipamentos de informática será punido com pena de prisão e multa de um a quatro anos e, se a intrusão causar prejuízos econômicos, aumentará de um terço para dois terços. Anteriormente, as penas aplicáveis eram reclusão e multas de três meses a um ano (BRASIL, 2021).

Dessa forma, além da legislação específica para crimes no campo virtual, também devem ser respeitados os princípios e direitos básicos estipulados na Constituição Federal de 1988. Portanto, permite o amparo sobre os direitos protegidos, enfatizando a dignidade humana e constitucionalidade das regras para lidar com o crime cibernético.

5 CONSIDERAÇÕES FINAIS

Baseado na problemática se atualmente existem leis suficientes para o combate legislativo dos cibercrimes, este trabalho demonstrou que ainda não existem leis suficientes baseados nos seguintes motivos: poucas leis para o setor, e sanções que não inibem a prática sobre os crimes virtuais. Por mais que o país dispõe de três leis totalmente focadas na internet, elas ainda precisam de mais formulações para que a população seja amparada corretamente.

Tratando nas leis, é perceptível que o país precisa criar uma sanção especializada sobre a prática do *phishing*, que se mantêm como ataque mais frequente no país desde dados de 2017, se agravando durante a pandemia do COVID-19. Pode-se destacar que essa lei poderia estar vinculada a LGPD, uma vez que os dados roubados pelos criminosos agora estão regidos nela.

Nesse sentido, a LGPD pode ser considerada um marco a ser adaptado para melhorar o processo de criminalização referente a conduta dos dados pessoais, ao mesmo tempo, foi observado que muitas leis possuem a conduta de violação de dados, cujos crimes estão diretamente relacionados aqueles dispostos no Código Penal.

Outro principal destaque negativo vai para a pena dos crimes virtuais, que eram de apenas 3 meses até um ano, e multa. Numa tentativa clara de melhorar essa situação, a Lei 14.155/2021 buscou aumentar a quantidade da pena possível nos crimes informáticos, porém, devido a promulgação da lei ser muito recente, ainda não é possível observar os impactos dela no combate ao crime.

O Direito brasileiro ainda caminha devagar quando se trata da criação de leis voltadas para prevenção de crimes virtuais, seja devido à dificuldade legislativa em relacionar os contextos e dificuldades que a informática traz para a análise jurídica, ou pela rápida atualização dos tipos de golpes ou de recursos informáticos utilizados que dificultam a criação de leis específicas.

Por isso, para futuras pesquisas, recomenda-se o estudo de projetos de leis voltados a internet, para verificar quais tipos de projetos estão em tramitação no senado, se remetem a atualização das leis existentes, criação de novas e como elas podem estar relacionadas ao combate ou prevenção do cibercrime e porque ainda não foram promulgadas, permitindo identificar a velocidade e a percepção e ação do Direito frente a está temática.

REFERÊNCIAS

AGRELA, L. Site falso do BB é quase convincente para roubar seus dados. **Exame**, 25 jul. 2019. Disponível em: https://exame.com/tecnologia/site-falso-do-bb-e-quase-convincente-para-roubar-seus-dados/ Acesso em: 16/06/2021.

AZEVEDO; J. S. de.; CARDOSO, T. M. **Crimes cibernéticos: evolução e dificuldades na colheita de elementos de autoria delitiva**. 2021. 25 f. Trabalho de Conclusão de Curso (Bacharel em Direito) – Una Bom Despacho, Bom Despacho. 2021.

BOTTINI, P. C. Alerta sobre lavagem de dinheiro e crimes digitais na pandemia. **Consultor Jurídico**, 18 mai. 2020. Disponível em: https://www.conjur.com.br/2020-mai-18/direito-defesa-alerta-lavagem-dinheiro-crimes-digitais-pandemia#sdfootnote1sym Acesso em: 16/06/2021.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto- Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Diário Oficial da União,** 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 16/06/2021.

_____. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da União,** 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 16/06/2021.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União,** 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16/06/2021.

_____. Lei nº 13.185, de 6 de novembro de 2015. Institui o Programa de Combate à Intimidação Sistemática (*Bullying*). **Diário Oficial da União,** 06 nov. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso: 16/06/2021.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União,** 14 ago. 2018. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso: 16/06/2021.

_____. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. **Diário Oficial da União,** 27 mai. 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso: 14/07/2021.

_____. Superior Tribunal de Justiça. **Recurso de *Habeas Corpus* 117.680 do Pará, em 2020**. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/858018754/recurso-ordinario-em-habeas-corpus-rhc-117680-pr-2019-0269333-5/inteiro-teor-858018764?ref=serp. Acesso em: 14/07/2021.

_____. Tribunal De Justiça Do Distrito Federal. **Ação Civil Pública Cível N. 0733785-39.2020.8.07.0001, Brasília 2020**. Disponível em: https://www.conjur.com.br/dl/decisao-lgpd-justica-determina-site.pdf. Acesso em: 14/07/2021.

BRITO, R. G. G.. Aplicabilidade das Normas Penais nas Condutas Ilícitas de Cyberbullying Cometidas em Redes Sociais na Internet. **Revista Esmat**., v. 5, n. 6. 2013.

CONTE, C. P.; Aspectos Jurídicos do Cyberbullying. **Revista FMU Direito**, v. 24, n. 34. 2010.

CORTELA, J. J. C. **Engenharia social no Facebook**. 2013. 44f. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) – Universidade Estadual de Londrina, Londrina. 2013.

CRUZ, D.; RODRIGUES, J. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Científica Eletrônica Do Curso De Direito**, ed. 13, jan. 2018.

GONÇALVES, J. R.; OLIVEIRA, L. R. G. A ineficácia da punibilidade do cyberbullying no Brasil. **Revista Educar Mais,** v. 4, n. 2, 2020.

JESUS, D. de; MILAGRE, J. A. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016

JORGE, P. G. **Fraudes na Internet**: Uma proposta de identificação e prevenção. 2007. 79f. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) – Faculdade Santa Maria, Recife. 2007.

KASPERSKY. **Brasileiros são maiores vítimas de golpes phishing no mundo**. 2018. Disponível em: <https://www.kaspersky.com.br/blog/phishing-klsec-brasil-assolini/10642/?utm_source=newsletter&utm_medium=Email&utm_campaign=kd%20weekly%20digest>. Acesso em: 21/06/2021.

LAS-CASAS, P. H. B. et al. Uma metodologia para identificação adaptativa e caracterização de phishing. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 34., 2016. **Anais...** Salvador: UFBA.

NASCIMENTO, S. de P. Cibercrime: conceitos, modalidades e aspectos jurídicos penais. **Âmbito Jurídico**, 3 set. 2019. Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais. Acesso em: 14/07/2021.

PEREIRA, L. de D.; MARTINS, D. M. S. Engenharia social: segurança da informação aplicada à gestão de pessoas – estudo de caso. **Caderno de Estudos em Sistemas de Informação**, v. 1, n. 2. 2014

RODER, P. C. S.; SILVA, H. M. da. **Crimes Cibernéticos**. Porto Alegre: Livraria do Advogado, 2018.

RODRIGUES, O. L. **Marco Civil e opção do legislador pelas liberdades comunicativas**. 2014. Disponível em: https://www.conjur.com.br/2014-mai-14/direito-comparado-marco-civil-opcao-pelas-liberdades-comunicativas. Acesso em: 16/06/2021.

SATAKE, M. **Conheça as fraudes digitais mais comuns na pandemia e veja como evitar**. 2020. Disponível em: https://invest.exame.com/mf/conheca-as-fraudes-digitais-mais-comuns-na-pandemia-e-veja-como-evitar. Acesso em: 14/07/2021.

SCHAU, G. Uma lista com 24 crimes virtuais. **JusBrasil**, 2019. Disponível em: https://guilhermebsschaun.jusbrasil.com.br/artigos/686948017/uma-lista-com-24-crimes-virtuais. Acesso em: 16/06/2021.

SILVA; R. L. da; VIEIRA, A. **Segurança cibernética: o cenário dos crimes virtuais no Brasil**. 2021. Disponível em: https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais. Acesso em: 16/06/2021.

SILVA, M. L. C. da.; et al. Legislativa na tipificação dos crimes cibernéticos e a sua intensificação com o aumento de usuários na internet em Goiás. **Praxis Jurídic@**, v. 5, n. 1. 2021.