FACULDADE EVANGÉLICA DE RUBIATABA
CURSO DE DIREITO
RICARDO AUGUSTO SOARES BIANGULO

CRIMES VIRTUAIS: A EVOLUÇÃO DA LEI E SEUS ASPECTOS PUNITIVOS

RUBIATABA/GO
2021

RICARDO AUGUSTO SOARES BIANGULO

CRIMES VIRTUAIS: A EVOLUÇÃO DA LEI E SEUS ASPECTOS PUNITIVOS

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba, sob orientação do professor Mestre Pedro Henrique Dutra

RUBIATABA/GO
2021

RICARDO AUGUSTO SOARES BIANGULO

CRIMES VIRTUAIS: A EVOLUÇÃO DA LEI E SEUS ASPECTOS PUNITIVOS

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba, sob orientação do professor Mestre Pedro Henrique Dutra.

MONOGRAFIA APROVADA PELA BANCA EXAMINADORA EM 23 / 08 / 2021

PEDRO HENRIQUE DUTRA
Mestre em Ciências Ambientais
Orientador
Professor da Faculdade Evangélica de Rubiataba

FERNANDO HEBERT DE OLIVEIRA GERALDINO
Especialista em Direito Público
Examinador
Professor da Faculdade Evangélica de Rubiataba

GLAUCIO BATISTA DA SILVEIRA
Especialista em Direito Tributário
Examinador
Professor da Faculdade Evangélica de Rubiataba

Dedico esse Trabalho de conclusão de curso para meus pais que são minha maior motivação, sempre me incentivando nas horas difíceis e me dando todo apoio possível.

AGRADECIMENTOS

A Deus e Nossa Senhora por me dar a vida, por me dar sabedoria e inspiração. E a São Bento que me protege de todo o mal.

Aos meus pais Maria Marcia e Marcio Biangulo, por sempre está comigo me incentivando e apoiando nas minhas fases da vida, me ensinando sempre ser honesto e correto com as coisas da vida.

A Laisa, minha namorada, companheira fiel e dedicada, na qual me espelho. Sempre me ajudando e me dando todo incentivo e suporte no decorrer do curso e na vida.

Ao Professor Ms. Pedro Henrique Dutra, o qual sempre compactuou comigo acerca do tema e das boas ideias, contribuindo de forma excepcional para este trabalho.

RESUMO

O Direito Digital trabalha para garantir a atualização jurídica e penal das leis para que se adaptem as novas situações que ocorrem com a população em meios informáticos. Ela é importante porque a internet traz inúmeros novos conceitos e tipificações que o Direito precisa buscar conhecimento continuo para que as pessoas não fiquem desamparadas, principalmente nos cibercrimes realizados na internet. Logo, o objetivo desta monografia é verificar a jurisprudência e doutrina aplicadas as leis que remetem proteção da população nos meios informáticos. Para atingimento deste objetivo o autor desenvolveu o estudo de revisão de literatura com abordagem qualitativa. Os arquivos lidos foram encontrados nas bases de dado *Google Scholar* onde foram selecionadas as principais leis, juntamente com artigos, periódicos online e livros, com língua portuguesa, com ano de publicação entre 1996 a 2021, sendo utilizados como descritores: cibercrimes, direito penal do cibercrime. Dessa forma, foi possível responder a problemática de como o Direito brasileiro contribui para atualização das leis e julgamento dos crimes cometidos em meio virtual? Foi possível verificar que o Direito Digital possui uma evolução contínua sobre diversos aspectos que podem estar direcionados as questões informáticas, como crimes exclusivamente na internet, que levou a Lei Carolina Dieckmann. O controle da privacidade e dos dados, que permitiram a criação do Marco Civil da Internet e da Lei Geral de Proteção de Dados. E da adaptação das leis existentes para também serem julgadas quando realizadas pela internet, como estelionato, assédio moral e pedofilia.

Palavras-chave: Cibercrime. Direito. Internet.

ABSTRACT

Digital Law works to guarantee the legal and penal update of the laws so that they adapt to the new situations that occur with the population in computer media. It is important because the internet brings countless new concepts and typifications that the Law needs to seek continuous knowledge so that people do not become helpless, especially in cybercrimes carried out on the internet. Therefore, the objective of this monograph is to verify the jurisprudence and doctrine applied to the laws that refer to the protection of the population in information technology. To achieve this objective, the author developed a literature review study with a qualitative approach. The files read were found in Google Scholar databases where the main laws were selected, along with articles, online journals and books, in Portuguese, with year of publication between 1996 and 2021, being used as descriptors: cybercrimes, criminal law of the cybercrime. In this way, was it possible to answer the problem of how Brazilian Law contributes to updating laws and prosecuting crimes committed in a virtual environment? It was possible to verify that the Digital Law has a continuous evolution on several aspects that may be directed to information technology issues, such as crimes exclusively on the internet, which led to the Carolina Dieckmann Law. The control of privacy and data, which allowed the creation of the Marco Civil da Internet and the General Data Protection Law. And the adaptation of existing laws to also be judged when carried out over the internet, such as embezzlement, moral harassment and pedophilia.

Keywords: Cybercrime. Law. Internet.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

O mundo globalizado é marcado pelo surgimento de tecnologias que promovem um alto nível de circulação de informações, pessoas e bens. A Internet é um exemplo marcante dessa era contemporânea, pois atinge a vida de milhares de pessoas e se tornou algo necessário para o cotidiano.

Com a evolução da Internet e todas as suas contribuições sociais, políticas, econômicas e jurídicas, surgiu o Direito Digital. Essa nova área permitiu a evolução do próprio Direito, abrangendo todos os princípios jurídicos básicos e instituições jurídicas que têm sido eficazes e aplicados até o presente, e introduzindo novas instituições e elementos de pensamento jurídico em vários outros campos (MAUES et al, 2018).

O Direito Digital também permite a atualização sobre os problemas que podem ocorrer em meio a toda usabilidade que a internet permite para a população no século XXI, os chamados crimes virtuais, que consistem em crimes realizados na internet. Como resultado, a lei precisa se adaptar a essa nova realidade para proteger os bens jurídicos e manter a dignidade humana.

No mundo digital, o desenvolvimento da Internet não trouxe apenas um progresso positivo. Os crimes virtuais se tornaram frequentes no mundo todo devido as condições que a internet gera de anonimato, e os diversos crimes se adaptaram e podem ser cometidos na internet. Logo, o desafio do sistema jurídico é responder com urgência a essa nova demanda legislativa. Porque é fundamental para o país se manter seguro em relação a legislação, uma vez os crimes virtuais geram situações que causam grandes prejuízos sociais, econômicos e psicológicos na população.

A problemática deste trabalho consiste em avaliar como o Direito brasileiro contribui para atualização das leis e julgamento dos crimes cometidos em meio virtual?

O objetivo geral escolhido foi de verificar a jurisprudência e doutrina aplicadas as leis que remetem proteção da população nos meios informáticos. Assim, os objetivos específicos são: descrever como consiste o cibercrime e como são os crimes virtuais que ocorrem no Brasil; descrever as principais leis voltadas ao meio informático no Brasil; entender como a jurisprudência brasileira trabalha nos diversos tipos de crimes virtuais possíveis.

A metodologia escolhida para o trabalho foi a revisão de literatura com abordagem qualitativa. Dessa forma, foram realizados estudos em bases de dados online para adquirir o levantamento bibliográfico necessário para responder a problemática, sendo organizados a partir do método dedutivo. O método dedutivo é importante porque parte do contexto de interpretação das leis e como elas são criadas para suprir a necessidade de proteção e prevenção de crimes realizados por meios informáticos.

Foi possível estabelecer o direcionamento da leitura para o tema geral do cibercrime e alterando para o foco de estabelecer a evolução do Direito frente as leis que o combatem. Os periódicos escolhidos foram encontrados nas bases de dado Google Acadêmico onde foram selecionadas as principais leis, juntamente com artigos, periódicos online e livros, ano de publicação entre 1996 a 2021 e em português.

No primeiro capítulo tem foco em apresentar as principais questões doutrinárias e históricas relacionadas aos crimes virtuais, para embasar como o Direito evoluiu para iniciar os processos jurídicos de adaptação da lei com atendimento desta nova demanda de proteção e amparo para população.

No segundo capítulo destaca as principais leis criadas no Brasil focadas exclusivamente para a internet, sendo descrito as leis Carolina Dieckmann (Lei nº 12.737/2011), o Marco Civil da Internet (Lei n o 12.965/2014) e a Lei Geral de Proteção de Dados (lei nº 13.709/2018) que destacam algumas das principais direcionamentos do uso da rede como crimes, privacidade e uso dos dados.

E no terceiro capítulo foram complementados como a jurisprudência trabalha nos casos de crimes informáticos e como a lei se adaptou em crimes não tipificados nas três principais leis da internet, como é o caso da adaptação do estelionato, pedofilia e outros crimes que tiveram mudanças nos já existentes artigos, verificando que a lei brasileira também busca adaptar crimes já existentes e que se tornaram frequentes nos meios informáticos.

2. DEFINIÇÃO DE CRIMES VIRTUAIS

Este capítulo permite introduzir o leitor sobre os contextos gerais estabelecidos sobre a temática de crimes virtuais. Como a pesquisa tem o foco em apresentar o contexto científico, doutrinário e jurídico existente nos possíveis tipos de crimes virtuais, além da evolução do Direito na criação de leis que protegem a população desses crimes, se faz necessário verificar as definições, origens e evolução deste tipo de crime na sociedade.

A explicação desse contexto também permite observar como os crimes virtuais se tornaram as principais ameaças frente as jurisprudências tradicionalistas, na qual o Direito precisou se adaptar de acordo com as temáticas enfrentadas. Ainda assim, demonstrando como o crime virtual consiste num meio vantajoso para os criminosos, não apenas na falta de amparo jurídico inicial que ela teve no seu histórico, mas também pelo anonimato da internet.

Um crime virtual nada mais é do que o uso de tecnologias para cunho criminoso ou qualquer comportamento realizado na internet, ou ciberespaço, que possua característica de um crime conforme a lei. Podem estar relacionados a crimes que violam direitos básicos, seja por meio do uso da tecnologia da informação para a realização de atividades criminosas ou em crimes com maior grau de perigo para a população (ALEXANDRE JUNIOR, 2019).

Para a maioria dos doutrinadores, o conceito de crime pode ser resumido como o comportamento de uma pessoa que viola a ética e a moral estipuladas pela lei, o que prejudica os interesses jurídicos da proteção proporcionada pela lei. Com o desenvolvimento da tecnologia, especialmente o desenvolvimento da Internet, os crimes representados pela legislação vigente do país se tornam mais vantajosos porque os legisladores não conseguem acompanhar essa evolução, o que faz com que a Internet perca fiscalização legislativa, portanto, se tornando o que chamam de “terra sem lei” (CHAUVET, 2016).

Essa nova categoria de delito também é conhecida como crime cibernético, digital, eletrônico, cibercrimes, fraudes eletrônicas, delitos computacionais ou de alta tecnologia, sendo considerados qualquer comportamento humano (omissivo ou comissivo) que usa um computador para realização de delitos para ganho próprio. Geralmente o crime é realizado buscando algum benefício ao infrator, mesmo que certos crimes não prejudiquem direta ou indiretamente a vítima (LUCCHESI; HERNANDEZ, 2018).

No ciberespaço, existem dois principais perfis que se destacam devido à riqueza de conhecimentos de informática: os hackers e crackers. Embora a presença de hackers pareça

estar relacionada à maioria dos crimes que ocorrem em ambientes virtuais, na verdade o cracker é o verdadeiro responsável, na qual a única diferença entre os dois está na forma como usam o conhecimento. Enquanto os hackers não tenham intenção de causar danos, os crackers agem buscando sempre vantagens ilícitas sobre as vítimas (SANCHES; ANGELO, 2018).

Para a doutrina brasileira, a definição dos crimes informáticos está descrita conforme a Lei n. 12.737, de 30 de novembro de 2012, em seu artigo 154-A, que alterou o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal, passando a valer a seguinte descrição:

> Art. 154-A. Invadir disposto informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismos de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" (BRASIL, 2012).

A nível criminal, a lei prevê detenção e multa que variam de 3 (três) meses a 1 (um) ano. Além disso, a referida lei alerta que tais penalidades incorrem em quem produz, fornece, distribui, vende ou distribui equipamentos ou programas de computador destinados a cometer atos criminosos. Também ocorre se ocasionar prejuízos econômicos e se a intrusão resultar no acesso ao conteúdo e se o crime se tornar grave, a pena de reclusão será severamente aumentada para o prazo de 6 (seis) meses a 2 (dois) anos, além de multa (ALEXANDRE JUNIOR, 2019).

Porém, devido ao aumento da criminalidade por meios informáticos, no momento, as leis voltadas à internet parecem surtir poucos efeitos de prevenção, principalmente porque o submundo do crime cibernético continua a crescer. Dentre os principais motivos que podem ser destacados sobre esse aumento, pode-se citar o baixo investimento no combate a esses crimes, a falta de segurança digital e falta de uma cultura voltada para a conscientização da comunidade de usuários, o que geralmente não é compreendido pelos setores público e privado (LEMOS, 2021).

Logo, percebe-se na nomenclatura dos crimes virtuais que se tratam de crimes que já existem na sociedade, porém, passaram a ser realizados na internet, com uso de meios informáticos, como computador, smartphone, dentre outros. Na lei brasileira, já é possível verificar a doutrina criada, na qual consiste em lei criada em 2012, atribuindo reclusão e multa para aqueles que praticam o crime neste formato.

Porém, após o conhecimento da definição do tema, é interessante observar o contexto histórico em que os crimes virtuais estão situados, verificando o seu início e como

ele está sendo aplicado hoje no Brasil. Assim é possível entender o porquê determinadas temáticas se tornaram tão praticadas no Brasil e como o Direito age para combatê-las.

2.1 A ORIGEM DOS CRIMES VIRTUAIS

Este subtópico permite entender como os crimes virtuais surgiram de fato. Sabendo que se tratam de crimes praticados na internet, então deve-se verificar como se deu esse desenvolvimento da internet, sua popularização e importância na vida das pessoas, destacando os motivos que a tornam ambientes propícios para a criminalidade.

Os crimes contra a informação já ocorriam antes da existência Internet, porém, devido ao crescimento contínuo da globalização, da liberdade de expressão, e das tecnologias de informática, os crimes virtuais se tornaram uma nova porta de entrada para os criminosos. Embora essas ferramentas tenham realmente se tornado indispensáveis hoje, ela pode virtualmente implementar crimes que foram estipulados na Lei Criminal, porém, fornecem novas oportunidades devido ao formato de aplicação que o crime está sendo realizado (BRITO, 2021).

Na história da internet, sua primeira nomenclatura foi a chamada ARPANET (*Advanced Research Projects Agency Network*), sendo desenvolvida nos Estados Unidos (EUA) no final dos anos 1960 como um meio mais seguro de comunicação entre militares e cientistas. O nome Internet surgiu nos Estados Unidos na década de 1970, quando o Departamento de Defesa dos EUA criou um sistema que ligava vários centros de pesquisa militar para permitir a transmissão de informações e dados. Isso só foi possível devido ao acúmulo de pesquisas em informática e ao desenvolvimento de computadores (MAUES et al., 2018).

Com a popularização da Internet com o decorrer das décadas, houve um foco crescente na proteção de dados confidenciais compartilhados por empresas e governos online. Na década de 1990, o termo cibercrime foi criado em plena reunião do G-8, em que foi definida a nomenclatura inicial da temática e uma pena prática do crime. Quando apresentado os motivos da criação dessas leis, destacaram a velocidade da realização do delito e o anonimato no compartilhamento de informações, sendo as principais características que dificultam o controle das atividades do usuário e o combate ao crime (D'URSO, 2017).

Desde meados da década de 1990, após cerca de 20 anos de avanço tecnológico, a Internet começou a mudar a sociedade. As pessoas começaram a consumir serviços de

informação, produtos e entretenimento, o que mudou as relações pessoais, familiares, profissões e negócios (CAMARGO, 2020).

No Brasil, foi no ano de 1988 que a internet recebeu seus primeiros investimentos nas cidades de São Paulo e Rio de Janeiro. Logo após, foi se desenvolvendo e se expandindo gradativamente até atingir todos os estados, e por causa do seu conceito, algumas leis de dados já foram criadas na própria Constituição Federal de 1988, tratando do respeito a proteção dos dados (CRUZ; RODRIGUES, 2018).

Essa atualização foi importante para complementar a lei 7.232/84, que dispõe sobre a Política Nacional de Informática e outras providências, sendo a principal lei que se manteve para a formalização de um crime virtual até a lei criada em 2012. Porém, no Brasil, mesmo diante da falta de leis relacionadas a crimes informáticos, cada lei era tratada conforme a sua prática, como em casos de assédio, roubos ou golpes, mesmo que fossem realizadas pela internet e o judiciário ainda não havia se atualizado (BRASIL, 1984)

É fato que o desenvolvimento da tecnologia da informação e a rápida integração de milhões de usuários da Internet em todo o mundo conectaram indivíduos dos mais diferentes países e culturas e mudaram a relação entre pessoas, regiões e empresas. A relação entre negócios, das transações bancárias e as relações sociais passaram a ocorrer em tempo real de forma mais acelerada, encurtando as distâncias e rompendo as barreiras do tempo e do espaço que existiam anteriormente (SANTOS, 2020).

Outro ponto criado com a internet foi o anonimato, sendo o principal motivo que levam os criminosos em criar estratégias para a pratica de crimes, na qual começou a desenvolver um estereótipo de que a internet não era um ambiente seguro. Logo, com a evolução da Internet e das tecnologias de forma avançada, tornava difícil lidar o judiciário tratar de todos esses crimes, porque o autor de um crime cibernético poderia ser qualquer pessoa que tenha conhecimentos de informática e seja proficiente em quebrar senhas (SILVA; PAVANI, 2016).

Esses crimes apresentam características de transnacionalidade, universalidade e ubiquidade, ou seja, tratam-se de delitos praticados em todo o mundo porque todos os países adquiriram e utilizam tecnologias da informação, independentemente de sua força econômica, estágio social ou modelo cultural. Logo, os crimes virtuais passam a ser classificados de acordo com o formato de aplicação. Podem ser classificados como próprios, ou seja, crimes cometidos apenas por meios informáticos e crimes impróprios, que são cometidos de qualquer forma, enquanto os dispositivos eletrônicos são apenas mais um meio de execução (AZEREDO, 2020).

Trazendo outros contextos sobre as classificações dos tipos de crimes virtuais, Marra (2019) apud Túlio Lima Vianna (2004) considera que os delitos virtuais se subdividem em quatro grupos, quais sejam:

> 1) Delitos informáticos impróprios: são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa à bem jurídica inviolabilidade da informação automatizada (dados).
> 2) Delitos informáticos próprios: são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).
> 3) Delitos informáticos mistos: são aqueles complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa. São os delitos derivados do acesso não autorizados a sistemas computacionais que ganharam "status" de delitos "sui generis" dada a importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos.
> 4) Delito informático mediato ou indireto: é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação (MARRA, 2019, p. 2019).

Observando esse contexto dos crimes virtuais, sua principal vantagem para os criminosos está no seu anonimato, ao mesmo tempo que as evoluções avançadas dessas tecnologias permitem que os malfeitores com conhecimento consigam agir com mais liberdade e possibilidade.

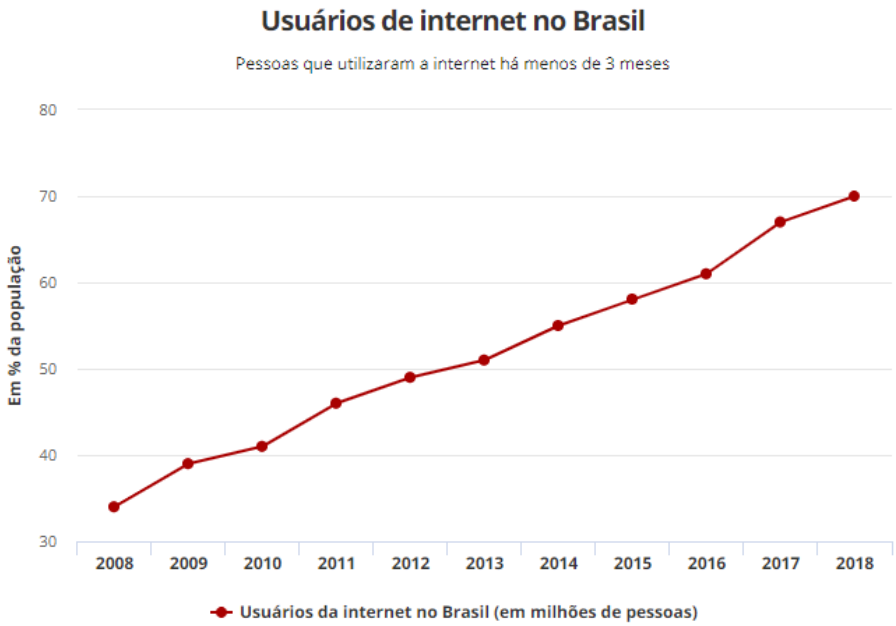
Dessa forma, entende-se o que é o crime virtual e o quais os motivos de seu crescimento e motivação para que alguém à realize. Nesse contexto, o próximo subtópico trata dos crimes virtuais no Brasil, estabelecendo como esses crimes estão situados no país e qual a atenção do Estado para o cuidado disso, cujas atualizações realizadas constam de forma detalhada nos capítulos 3 e 4.

2.2 OS CRIMES VIRTUAIS NO BRASIL

O mundo vive a chamada Era Digital, onde todos (crianças, jovens, adultos e idosos) estão conectados na Internet, trazendo inúmeras formas de comunicação, entretenimento, trabalho e consumo de produtos e serviços. No Brasil, pesquisa realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE) em 2017 mostrou que 74,9% da população brasileira tem acesso à rede no país (IBGE, 2018).

Essa capacidade de aumento do acesso à internet brasileira caminha por passos largos, pois num período de dez anos, a porcentagem da população que possui algum tipo de acesso a internet, seja por computador, celular, ou outro tipo de equipamento mais que dobrou, conforme pode ser observado na Figura 1.

Figura 1 – Acesso à internet pela população brasileira entre 2008 a 2018



Fonte: Lavado (2019).

Devido a esse desenvolvimento, os recursos disponíveis na Internet (como redes sociais e outras plataformas de comunicação) cresceram exponencialmente, portanto, o número de indivíduos navegando na tecnologia aumentou. Com a quantidade de pessoas conectadas, esse ambiente se torna propícia a comportamentos ilegais, como a divulgação de informações e conteúdo sexual sem o consentimento das vítimas, golpes, estelionato, abuso, dentre outros (AZEREDO, 2020).

De acordo com uma pesquisa realizada pela Equipe da Trend Micro em 2015 sobre "*Raising Ranking: Brazilian Cybercriminals*", em tradução direta "Ranking de avaliação: Cibercriminosos brasileiros", apesar do desenvolvimento de ferramentas, o número de cibercrimes no Brasil ainda está amadurecendo, adotando proprietário ou Estratégia. Há evidências de que o Brasil é um dos cinco países que mais sofrem crimes cibernéticos, ocupando o primeiro lugar na América Latina. Talvez o que torna este mais propício aos ataques de cibercriminosos brasileiros que aproveitam as oportunidades oferecidas por redes sociais como Facebook, YouTube, Twitter, Instagram e Skype (LEMOS, 2021).

> Os ambientes "virtuais" – como sites de busca, de redes sociais, dos provedores de acesso e de conteúdo, as propagandas que permeiam os milhares de sites na web –, são propícios para condutas perniciosas de pedófilos e criminosos de todos os matizes, podendo desembocar em crimes como calúnia, difamação, injúria, ameaça,

> pornografia infantil, induzimento ao suicídio, falsa identidade, fraudes, que acabam atingindo crianças e adolescentes, ainda em fase de formação física, psíquica e emocional (SANTOS, 2020, p. 158).

Infelizmente o Brasil é um dos países mais afetado do mundo sobre os ataques cibernéticos, em especial nos ataques de *phishing*. Por se tratar do ataque mais comum voltado para realização de golpes e roubo de dados, 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 dos usuários mais rápida e eficaz. Possivelmente, mesmo que um ataque ainda não tenha chegado ao país (CAMARGO, 2020).

Depois de roubar com sucesso os dados do usuário, eles serão vendidos para cidadãos brasileiros e qualquer pessoa interessada no mundo, como números de celular e de casa, endereço completo, nome completo do CPF, números de identificação em sites específicos. Pode-se citar o site de divulgação de dados pessoais para brasileiros www.tudosobretodos.se. Seu nome de domínio está localizado na Suécia e não no Brasil. Por isso, apesar das tentativas de banir o site, ele ainda está sob a responsabilidade do Ministério Federal de Relações Públicas (LEMOS, 2021).

Quando não é a venda de dados da população, pode-se ocorrer o vazamento, como foi ocorrido em 22 de janeiro de 2021, conforme apresentado pelo Instituto de Referência em Internet e Sociedade (IRIS), na qual mais de 220 milhões de brasileiros tiveram seus dados expostos na internet, inclusive contendo dados de pessoas falecidas. Neste caso, a venda ilegal teve forte especulação de que o site Serasa Experian, focado em informações de crédito e apoio a negócios do Brasil, foi o principal autor da venda e da origem dos vazamentos, por possuir o porte para comportar todos esses dados, mas não foi comprovado (IRIS, 2021).

Finalizando este capítulo, ele foi fundamental para situar a leitura estruturada do tema sobre as principais características que remetem os crimes virtuais, entendendo suas características e definições, qual seu histórico e porque se torna vantajoso para práticas ilícitas e, focando no Brasil, quais os principais crimes que podem ser cometidos.

Logo, verifica-se que o Brasil sofre inúmeros tipos de crimes virtuais, como *phishing*, danos contra a moral, estelionato, fraudes, perseguição, venda ilegal de dados, dentre outros, no entanto, é interessante observar que o país busca combater e regulamentar estes crimes, como será observado no capítulo seguinte, destacando as principais leis menores e maiores sobre as estratégias jurídicas para o combate aos crimes virtuais, principalmente em

relação da explicação da Lei Carolina Dieckmann, do Marco Civil da Internet e da Lei Geral de Proteção de Dados.

3 AS PRINCIPAIS LEIS NA PARA PROTEÇÃO DA INTERNET BRASILEIRA

Este capítulo tem como finalidade expor as características sobre as leis criadas para amparar as questões de informática do país. O Brasil é um país que passou por poucas mudanças realmente efetivas na área de informática, principalmente em relação a crimes virtuais onde ainda não existe uma legislação condizente com o recomendado (CHAUVET, 2016).

Porém, em relação a privacidade e ao controle de dados, e pelo menos na caracterização do que são os crimes virtuais, existem três leis que se destacam entre as demais e foram organizadas entre os subtópicos deste capitulo. É importante lembrar que para que determinada lei seja criada, é necessário que seja proposto um projeto, meio pelo qual nascerá a lei, tal projeto precisa passar por uma trajetória longa, demorada e complexa. Em síntese, o projeto percorrerá o Congresso Nacional, que é formado pela Câmara dos Deputados e pelo Senado, sendo finalmente aprovado pelo Presidente da República (MEDEIROS, 2018).

No Brasil, a primeira lei a tratar do assunto de informáticos foi criada antes mesmo da Constituição Federal 1988, no ano anterior ao fim do Regime Militar, a Lei nº 7.232/84 que dispõe sobre Política Nacional de Informática. A ideia da lei era instituir um reserva de mercado para fabricantes nacionais de produtos de informática, beneficiando-os com incentivos fiscais a fim de competir com grandes fabricantes internacionais. Esta lei serviu como meio de incentivo para o desenvolvimento e afloramento do interesse dos brasileiros aos assuntos informáticos (BRASIL, 1984)

A Lei nº 9.296/96 regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal, que disciplina a interceptação de comunicação telemática ou informática. O tema da lei até os dias atuais é polêmico devido à divergência existente entre a limitação dos direitos fundamentais envolvidos no durante uma intercepção, como a privacidade e intimidade, e a segurança da população gerando questionamentos sobre sua inconstitucionalidade (BRASIL, 1996)

A Lei nº 9.609/98 trata da proteção da propriedade intelectual do programa de computador além de sua comercialização no país. Como consequência da legislação supracitada surge a Lei 9.610/98, que trata direitos autorais, além dos advindos dos programas criados a fim de evitar pirataria, tanto no meio virtual (crime cibernético) como no real (BRASIL, 1998).

A Lei nº 9.983/2000, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública. Tal lei acresceu à Parte Especial do Código Penal o artigo 168-A, crime cibernético de apropriação indébita; artigo 313-A E 313-B tratam de crimes contra o sistema previdenciário; além de alteração na redação dos artigos 153, 296, 297, 325 e 327 do Código Penal, os quais tratam em síntese de banco de dados (BRASIL, 2000).

Em 2008, entrou em vigência a Lei nº 11.829/2008, a qual alterou a redação dos artigos 240 e 241, acrescentando ainda os artigos 241-A, 241-B, 241-C, 241-D, 241-E na Lei no 8.069/90 - Estatuto da Criança e do Adolescente, a fim de aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet (BRASIL, 2008).

E assim, entendendo que o Brasil sempre realizou pequenas alterações nas leis para tentar se adequar as possíveis situações jurídicas frente a crimes virtuais, as três leis que devem ser destacadas durante esse capítulo são a Lei Carolina Dieckmann, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais.

3.1 LEI Nº 12.737/2012 - LEI CAROLINA DIECKMANN

A criação do projeto que deu origem a Lei nº 12.737 se deu no ano de 2011, quando a atriz Carolina Dieckmann foi vítima de tentativa de extorsão, sendo chantageada e ameaçada por indivíduos que continham em seu poder imagens íntimas da atriz. Tais imagens haviam sido furtadas de seu computador após um e-mail ser usado como isca (spam), que ao ser aberto liberou uma porta para a instalação de um programa que permitiu aos crackers acessarem todo conteúdo presente no computador da atriz (G1, 2012).

Os indivíduos que a ameaçaram tinham como finalidade receber um valor em troca das imagens não serem publicadas na internet, porém após não ceder às chantagens suas fotos foram publicadas em vários sites. Após investigação a polícia conseguiu chegar aos autores do crime, pois assim como a maioria dos crimes ocorridos no meio ambiente real, os crimes ocorridos no meio virtual também deixam rastros. No entanto, devido à ausência de lei especifica para punir os envolvidos estes foram indiciados por furto, extorsão qualificada e difamação (G1, 2012).

Por fim, a Lei 12.737/2012 tipificou a invasão dos dispositivos informáticos ocorridas no Brasil, atribuindo pena, consoante ao artigo 154-A do Código Penal, para as

situações de violação de mecanismo de segurança que vislumbram a obter, destruir ou adulterar dados ou informações sem autorização do titular do respectivo dispositivo. A finalidade é de proteção à privacidade e, consequentemente, à intimidade e à vida privada do indivíduo. É, pois, de competência Estadual o crime em análise, que será processado mediante a representação do ofendido no local onde ocorreu a invasão (por ser um delito formal, não se exige o resultado), o que será excepcionado na hipótese de cometimento contra algum ente da União (BRASIL, 2014)

O artigo 4º da lei estipula "Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado", ou seja, a criação de setores de combate ao crime virtual nas delegacias comuns e delegacias especializadas em crimes eletrônicos (MAUES et al., 2018).

A Lei Carolina Dieckmann foi elogiada no meio jurídico devido a possibilidade de garantia da privacidade e intimidade das pessoas que podem ser expostas a este tipo de crime. Porém, uma das críticas que a lei recebeu foi devido à demora do judiciário em aprovar esse tipo de lei, porque o crime em si estava se tornando comum na época, só recebendo a devida atenção depois que alguém famoso passou por esse tipo situação (DONEDA, 2019).

Para a sociedade, de certa forma, existe o descontentamento com essa situação, pois em muitos casos, a segurança dos dados pessoais é violada por negligência legal, e o tratamento frente a está segurança é fraco. Vale ressaltar também que a pena pode ser considerada leve, pois há detenção, e somente em termos de qualificação penal pode haver reclusão (MAUES et al., 2018).

E, assim, o Ministério Federal mencionou que em um ambiente cibernético, as várias possibilidades de ocultação de identidade, como o uso de perfis falsificados, são difíceis de combater os crimes cibernéticos devido aos obstáculos para a identificação dos criminosos. Para buscar controle sobre esse tipo de problema, foi desenvolvido o chamado Marco Civil da Internet, sendo o primeiro marco legislativo a proteger os direitos fundamentais de privacidade e liberdade de expressão no mundo virtual (VOINAROVSKI; MAGALHAES, 2018).

3.2 LEI Nº 12.965/2014 - MARCO CIVIL

A legislação brasileira também determinou, através da Lei n. 12.965/2014 (Marco Civil da Internet), "princípios, garantias, direitos e deveres para o uso da Internet no Brasil". Entre seus artigos, consta a responsabilização do provedor de internet, que disponibiliza conteúdo de imagens, de vídeos e de outros materiais contendo nudez e atos sexuais privados de terceiros, que violem a intimidade, sem a autorização dos participantes, não indisponibilizando o conteúdo após recebimento de notificação legal.

> O art. 3º do Marco civil da internet prevê que no Brasil ela se encontra alicerçada em um tripé axiológico formado pelos princípios da neutralidade de rede, da privacidade e da liberdade de expressão, que **estão** ligados entre si. Enquanto a neutralidade de rede reforça a liberdade de expressão, a privacidade representa seu limite (BRASIL, 2014).

A legislação brasileira também estabeleceu, por meio da Lei n o 12.965/2014 (Marco Civil da Internet), "princípios, garantias, direitos e deveres para o uso da Internet no Brasil". Entre seus artigos, consta a responsabilização do provedor de internet, que disponibiliza conteúdo de imagens, de vídeos e de outros materiais contendo nudez e atos sexuais privados de terceiros, que violem a intimidade, sem a autorização dos participantes, não indisponibilizando o conteúdo após recebimento de notificação legal.

> 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. §1º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação. §2º Não há crime quando o agente pratica as condutas descritas no caput deste artigo em publicação de natureza jornalística, científica, cultural ou acadêmica com a adoção de recurso que impossibilite a identificação da vítima, ressalvada sua prévia autorização, caso seja maior de 18 (dezoito) anos.

Dessa forma, quanto aos mecanismos sociais que podem ser utilizados para ajudar as vítimas, é importante destacar que além do judiciário, ministérios públicos e polícias militar e civil, o Brasil também conta com a atuação de organizações não governamentais, que atuam como um papel muito importante. Desempenham um papel importante no combate, protegendo e auxiliando as vítimas, pois os danos causados devem ser amparados. Assim, a legislação brasileira sobre crimes virtuais pode ser evoluída, especialmente quando

comparado aos anos em que existiam lacunas na proteção dos internautas e melhorias no uso adequado da tecnologia (CAMARGO, 2020).

Porém, outro grande problema quando se trata de investigação de crimes digitais remete a necessidade de obter dados que estão criptografados, como ocorre nos aplicativos de comunicação como o WhatsApp. Na *Deep Web*, que costuma ser o ambiente mais utilizados pelos criminosos, essa dificuldade é maior, pois necessita da identificação de inúmeros dados informáticos para que o criminoso seja identificado e possa ser julgado, alguns desses dados necessários são os chamados log (histórico de registros), *cookie* (dados básicos do computador), e endereço MAC (identificador da placa de rede, cujo valor é único por placa) (LEMOS, 2021).

Nesse sentido, Fernandes e Cardi (2017) também complementam que

> A criação e distribuição gratuita de programas como o TOR agravaram o problema (*Onion Router*), que permite que as pessoas participem de "redes paralelas" conhecida como "*Deep Web*". Além disso, o desenvolvimento da tecnologia 3G e 4G para smartphones, que estão se tornando o principal meio de comunicação, tornam possível a mobilidade da aquisição e distribuição ilegal de materiais ilícitos (FERNANDES; CALDI, 2017, p. 105).

É claro que a ilegalidade recebe atenção investigativa, mesmo diante do aumento da possibilidade de criminalidade, tanto as leis quanto as agencias responsáveis por investigar cibercrimes estão em constante avanço para estabelecer o melhor cuidado jurídico e penal para amparar as vítimas e julgar os culpados. Uma delas, que torna a chamada *Deep Web* como ambiente mais propicio para ilegalidade no Brasil é a Lei de Proteção de Dados, que torna todas as empresas passíveis de controle adequado dos dados de seus usuários cabendo questões penais em casos de uso irregular ou criminoso dos dados das pessoas (LEMOS, 2021).

Conhecida pela Lei nº 13.709 foi criada em 2018 para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados. Tal lei abrange forma explicita em sua redação a proteção aos fundamentos antes previstos apenas na Constituição Federal, como a inviolabilidade da intimidade, da honra e da imagem, respeito á privacidade etc. (BRASIL, 2018).

Porém, no ano de 2019 o novo governo realizou reforma na redação da lei supracitada, inicialmente modificando o nome, sendo Lei Geral de Proteção de Dados Pessoais (LGPD) e em seguida modificando artigos e normas de acordo com a atual política do país. Insta salientar, que a lei tem prazo para vigência em vinte e quatro meses, portanto

ainda não está completamente em vigor, vigorando apenas os artigos que tratam da Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018).

3.3 LEI Nº 13.709/2018 - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Conforme Eduardo Tomasevicius Filho (2016) demonstra em sua obra, embora o Marco Civil da Internet seja amplamente elogiado por ser a primeira lei do mundo a regulamentar os direitos e obrigações dos usuários da Internet, ele não perceberá mudanças substanciais porque na verdade não acrescenta nada à legislação atual. As expectativas decorrentes da discussão desta lei decorrem da falsa crença de que a Constituição Federal, Código Civil, Código Penal, Código de Processo Civil e Criminal, Código de Defesa do Consumidor, Direito da Criança e Lei de Interceptação da Juventude e Comunicação (Lei nº 9.296 / 96) não se aplicam às relações jurídicas estabelecidas na Internet.

Por isso houve a necessidade da criação da Lei de Proteção de Dados, que serve "como um sistema baseado em etiquetas, permissões ou proibições para o uso de informações específicas, sem levar na devida conta os riscos objetivos potencializados pelo tratamento informatizado das informações pessoas" (DONEDA, 2019, p. 50).

Assim, essa lei estabelece a regulação de como os dados pessoais das pessoas devem ser tratados na internet, alterando os artigos 7 e 16 do Marco Civil da internet. Mesmo sendo aprovada em 2018, sua vigência só teve início em agosto de 2020. Esse tempo foi estabelecido para que as empresas pudessem se adequar as novas regras que entrariam em vigor, ao mesmo tempo, para o Direito, permitiu determinar os conceitos jurídicos sobre os dados pessoais sensíveis da internet (BRASIL, 2018).

Os dados pessoais sensíveis referem-se toda informação referente a pessoa, seja da raça ou origem étnica, crenças religiosas, opiniões políticas, filiação a sindicatos ou organizações de natureza religiosa, filosófica ou política, dados relacionados com saúde ou vida sexual, dados genéticos ou biométricos, que se relacionam com os dados pessoais da pessoa. Assim, o uso anônimo dos dados que impedem a identificação se torna meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Dentre os principais dados sensíveis que são levados em consideração para o controle e a gestão das empresas, evitando problemas com a LGPD, são: nome completo, CPF, RG, nacionalidade, estado civil, profissão e escolaridade. (CASTRO, 2019).

Dessa forma, este capítulo permitiu destacar as principais leis criadas voltadas totalmente para a internet, sendo direcionada ao combate de crimes e do controle dos dados da população e como eles são usados na internet, buscando garantir a autonomia das pessoas e sua segurança pessoal.

Logo, observa-se que no Direito brasileiro busca mudanças nas suas leis para estabelecer uma conduta de proteção e prevenção aos crimes cometidos por meios informáticos, sendo consideradas três principais leis para atender a essa demanda. Porém, quando observado a quantidade possível de crimes que podem ser cometidos na internet em relação as leis voltadas para o combate, o Direito ainda caminha em passos curtos, muita das vezes tentando alterar leis existentes para combater determinados crimes, conforme observado no capítulo a seguir.

4 DOS CRIMES VIRTUAIS E A CONDUTA NO JUDICIÁRIO

No entendimento das principais informações das criadas exclusivamente para a internet e na prevenção de cibercrimes, ao mesmo tempo que também se entende a doutrina e quais as características protetivas das principais leis informáticas criadas no Brasil, é possível partir para a conduta jurídica.

Sabe-se que a conexão à internet se tornou um padrão na vida humana. As pessoas estão cada vez mais conectadas e utilizando aplicativos, serviços, compras, redes sociais, dentre outros meios na qual podem ser vítimas de pessoas mal-intencionadas. Seja acessando Facebook, e-mail, telefone, videoconferência ou operando negócios bancários.

Junto a isso, o contexto básico da Constituição Federal de 1988, apresentado em seu artigo 5º, que trata dos direitos e garantias fundamentais, sendo a vida como primeiro bem inviolável, portanto, o indivíduo que violar tal bem-estará cometendo crime. O crime pode ser conceituado como uma violação de bens jurídicos protegidos, e este ato ilegal é praticado por um sujeito injusto que é punido pelo Estado por tentativa ou direcionamento dos bens protegidos, e a vida é a parte principal do sistema jurídico (BRASIL, 1988).

Mesmo diante disso, os crimes virtuais ainda ocorrem, levando o Brasil a um dos países do mundo mais acometidos a este tipo de crime. Logo, o foco dos subtópico deste capítulo será de formalizar o embasamento teórico e doutrinário sobre cada tipo de crime relacionado a sua realização em meios informáticos, e apresentar casos da jurisprudência para verificar como o âmbito jurídico definiu e tratou cada caso.

Isso é importante para demonstrar como o combate aos crimes virtuais é realizado, pois de nada significa uma lei se não for aplicada no âmbito penal para aplicar as devidas sanções aos infratores. Além disso, essa explicação permite responder com clareza as principais atribuições das leis em relação a sua característica judicial aplicada em casos reais.

Entende-se também das limitações dos direitos básicos envolvidos durante a possibilidade de interceptação (como privacidade e intimidade) e a segurança da população nos casos de crimes informáticos, mesmo assim, as leis estão cada vez se atualizando mais rápido para adotar uma dimensão de combate que diminuía a sensação de impunidade que os criminosos possuem.

No entanto, por não haver uma lista descritiva de condutas e, principalmente, por não haver legislação específica para a configuração dos crimes que podem ser realizados no

ciberespaço, é necessário recorrer ao disposto no Direito Penal, que não possui requisitos específicos para esta categoria. Nessa linha de pensamento, pode-se considerar como principais tipos de crimes virtuais: estelionato, crimes contra a honra, cyberbullying, e crimes que se relacionam a pornografia infantil (CNJ, 2018).

No que tange a questão de competência e avaliação do delito, o Código Penal determina em seu artigo 69 que será vistoriado: "I- o lugar da infração; II - o domicílio ou residência do réu; III - a natureza da infração; IV - a distribuição; V - a conexão ou continência; VI - a prevenção; VII - a prerrogativa de função" (BRASIL, 1941).

No CPI (2016), ficou comprovado que a aplicação destas questões afins é uma regra geral, pois não existe lei contrária para o conteúdo que se aplica à regra geral. Concluiu, ainda, que nos casos investigativos também se aplicará o Direito Comum, devendo as polícias federal e estadual cumprir o disposto no artigo 144, parágrafo 1º da Lei nº 10.446, de 2002, que avalia a apuração dos casos para resolução de infrações penais interestadual ou internacional.

Em questões de crimes virtuais, os Tribunais Superiores já têm decidido inúmeros conceitos e pensamentos para o julgamento dos diversos tipos de crimes virtuais, permitindo avaliar como a lei impacta na decisão e quais as estratégias utilizadas pelos juízes para determinar a pena adotada pelo réu nos tipos de crimes abaixo.

4.1 ESTELIONATO

O estelionato, ou fraude na Internet tem se tornado muito frequente. Os casos mais comuns nesse tipo de conduta ocorrem através de pessoas mal-intencionadas que reproduzem sites de vendas falsificados com desinformação para induzir as pessoas a pagar por produtos inexistentes (CRUZ; RODRIGUES).

Quanto à definição de fraude, ela é tratada no artigo 171 do Código Penal:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis (BRASIL, 1940).

De acordo com o ISP (Instituto de Segurança Pública) do Rio de Janeiro, no ambiente digital, os casos de fraude na Internet aumentaram de 11,8% para 24,3% durante a

quarentena do COVID-19 (NASCIMENTO, 2020). No estado de Minas Gerais, dados da Polícia Civil indicam que o número de crimes cibernéticos registrados em 2020 aumentou em 50% em relação aos dados do ano passado. Na Amazônia, em comparação, o número de casos no Departamento de Polícia de Interação com Polícia Civil do Estado aumentou em impressionantes 216% se comparado ao mesmo período de 2019 em relação a estelionato virtual (BRANDÃO, GLASMEYER, 2021).

Em caso avaliado pela 4° Vara Criminal de Curitiba em 2016, pela desembargara Sônia Regina de Castropenal, foi realizado o inquérito policial para busca e apreensão de equipamentos de informática devido ao crime de estelionato que estava sendo realizado em ambiente cibernético. Porém, foi observado nesta ementa um dos problemas do combate ao cibercrime, uma vez que o procedimento foi negado por constar a falta de provas para continuação do processo.

Outro caso, ocorreu na Comarca de Aparecida de Goiânia, em 2020, pelo relator Eudelcio Machado Fagundes, dessa vez negando Habeas Corpus de criminosos que haviam praticado o golpe de estelionato devido a coleta de dados das vítimas através de um site clonado do Detran-GO.

Após uma investigação longa, contínua e trabalhosa, o paciente foi identificado como o suposto autor do crime. Antes que a promotoria concordasse em representar as autoridades policiais, pacientes eram detidos preventivamente por supostas violações de equipamentos de informática e fraude ideológica (CP, arts. 154-A, § 3° e 299).

Devido as dificuldades do combate, junto ao aumento dos casos de estelionato devido a pandemia, está em tramitação do judiciário o Projeto de Lei 3376/20, que visa a adição do texto no art. 171 de forma que estabeleça mais diversificação e entendimento sobre os crimes de fraude, visando também no aumento da pena, conforme disposto abaixo:

> "Art. 171. Estelionato virtual § 6º Aplica-se pena em dobro se o crime for cometido mediante a invasão, adulteração ou clonagem de aplicativo de mensagens instantâneas e chamadas de voz para Smartphone ou com o emprego da rede de computadores, dispositivo de comunicação ou sistema informatizado." (BRASIL, 2020).

Dessa forma, é importante observar a que os legisladores estão cientes da necessidade de melhoria dessa lei, já estabelecendo em tramite um projeto de lei atual para estabelecer as definições adequadas para melhorar o combate a este tipo de crime. Ao mesmo tempo, é interessante reforçar no caso citado da Comarca de Aparecida de Goiânia, que a

clonagem do site do Detran-GO para obter os dados pessoais das vítimas se configura como *phishing*.

O *phishing* tem como principal objetivo nesses casos o roubo de dados pessoais e fraude em cartão de crédito. Nesse caso, os cavalos de Tróia são a principal ameaça, que está relacionada a técnicas baseadas em *phishing*. Os cavalos de Tróia são populares e usados para roubar credenciais de usuários, incluindo envenenamento de DNS, janelas de navegador falsas, extensões de navegador mal-intencionadas e proxies mal-intencionados.

Em todas as tentativas de golpe de *phishing* modernos, o código usado para gerar as páginas falsas vem de algum site real, geralmente a clonagem de bancos tem de ser a mais requisitada. Esta ação pode ser detectada várias vezes com soluções de segurança, às vezes ao tentar navegar para o site do seu banco ou da operadora de cartão de crédito, às vezes pode ajudar os pesquisadores a encontrar novas páginas falsas e adicioná-las para enviar vítimas para a rede (LEMOS, 2021).

Independente do formato usado, todos se configuram como fraude ou estelionato, logo, existe lei que pode ser usada para o julgamento, mesmo que adaptada para atender a demanda de ataque virtual. Porém, não muda o fato que o Direito Penal já está buscando a atualização desta lei para estabelecer o estelionato cibernético.

4.2 CRIMES CONTRA A HONRA

Os crimes contra a honra podem ser classificados em objetiva e subjetiva. Na objetiva se refere à maneira como as pessoas veem alguém e a subjetiva se refere à maneira como as pessoas se veem. Ao comprometer a honra subjetiva, os indivíduos começam a se ver da maneira como seus agressores se apresentam aos outros. É comum que uma pessoa publique fotos ou vídeos de outras pessoas sem a permissão de terceiros para se vingar ou por preconceito e ódio (BRITO, 2021).

O Código Penal descreve os principais crimes contra a honra, como calúnia, difamação e injúria:

> Art. 138 – Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena – detenção, de seis meses a dois anos, e multa […]
> Art. 139 – Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena – detenção, de três meses a um ano, e multa […]
> Art. 140 – Injuriar alguém, ofendendo lhe a dignidade ou o decoro:
> Pena – detenção, de um a seis meses, ou multa. […] (BRASIL, 1940)

Entendendo as leis que remetem ao crime contra a honra, percebe-se que ele também não está adaptado para a versão virtual, sendo passível de entendimento dos responsáveis pelo julgamento. Em caso realizado na 4° Câmara Cível do Tribunal de Justiça de Goiás (TJGO), apelação n° 0379852-93 pelo relator Delintro Belo de Almeida Filho, em 2020, foi realizado a indenização por danos morais devido a publicação de conteúdo ofensivo na internet contra agente público.

Na explicação sobre os motivos, destaca-se que embora o direito à liberdade de expressão seja protegido pela Constituição Federal, ele não é absoluto, restringe os direitos individuais e encontra o asilo constitucional em igualdade de condições. Ao mesmo tempo, é punido com a violação dos direitos da personalidade (BRASIL, 2020).

Outro caso ocorrido na 6ª Câmara Cível no TJGO, Apelação Cível nº 0066760.87, Desembargador Jeová Sardinha de Moraes, ocorrido em 2019, pessoa recorreu contra o caso de reparação de danos morais ajuizada, uma vez que a apelante anteriormente havia causado discurso de ódio e difamação em grupos e na página da empresa de veterinária e produtos agropecuários.

O desembargador deu o parcial provimento e redução da multa por danos morais, considerando o fato da apelada ser pessoa jurídica, logo, não possui honra subjetiva e estaria imune a aspectos de honra e autoestima. Dessa forma, é possível observar que aquilo que é escrito na internet pode ser usado contra a pessoa sobre o pretexto de injuria, difamação ou calunia.

É importante que a apelante esteja ciente também que a realização de processo sendo pessoa jurídica abre brechas para apelação civil, uma vez que pessoa jurídica está imune do contexto de crimes contra a honra. Ao mesmo tempo, é importante observar que existem casos que podem ser desprovidos, se levar em consideração a conduta de liberdade de expressão, porque é um dos direitos fundamentais da Constituição Federal de 1988, e geralmente o provimento ocorre mediante análise e verificação do contexto pelo desembargador.

O próximo caso também é um tipo de problema que afeta gravemente aqueles que são afetados, principalmente os jovens, sendo um problema que já é sério no seu formato presencial, e agora existe a versão no ciberespaço, o *cyberbullying*.

4.2.1 CYBERBULLYING

O *bullying* é um problema que ocorre principalmente nas escolas, que implica diretamente na condição psicológica e social dos jovens, sendo um dos problemas que necessitam de intervenção constante para o seu combate. Mesmo diante de todos esses impactos individuais e sociais, o *bullying* em si não possui tipificação de crime no Brasil, porém, suas ações podem configurar crimes de assédio moral, agressão, calúnia, difamação e injúria, dependendo de cada caso e dos eventos que foram realizados (NASCIMENTO, 2019).

No caso de *bullying* ocorrido online, também conhecido como *cyberbullying*, que é realizado principalmente nas redes socais, onde as vítimas podem salvar as telas das conversas realizadas para comprovar a difamação, possibilitando a materialização do crime. Com isso, a vítima pode buscar ajuda, registrando o ato infracional e dependendo da idade da vítima, também pode se relacionar com o Estatuto da Criança e do Adolescente (BRITO, 2021).

Nesse sentido, o *cyberbullying* é considerado como o "envio de mensagens, fotos ou vídeos por meio de computador, celular ou assemelhado, bem como sua postagem em "blogs" ou "sites", cujo conteúdo resulte em exposição física e/ou psicológica a outrem" (BRASIL, 2010).

O bullying é caracterizado conforme a lei n° 13.185/2015, em seu artigo 2 onde considera qualquer violência física ou psicológica em atos de intimidação, humilhação ou discriminação. Infelizmente, na lei não descreve uma sanção penal sobre quem pratica esse ato, porém, nesse caso conforme descrito anteriormente, a vítima pode recorrer como um crime contra a honra.

O *cyberbullying* inclui muitos métodos, tais como: perseguição online, *cyberstalking*, incitação ao sexo e pornografia. Perseguição online se trata de qualquer assédio em uma rede social, incluindo mensagens frequentes, comentários indesejados e assédio à vida pessoal. No *cyberstalking*, devido ao distanciamento da vítima e a proteção do anonimato pela possibilidade de criação de um perfil na rede sem identificação, o mesmo recorre a diversos atos de calunia e difamação contra a vítima, que pode sofrer psicologicamente nestes atos (VOINAROVSKI; MAGALHAES, 2018).

Para exemplificar o tratamento desses casos, escolheu-se a apelação nº 1094247-20.2018.8.26.0100, de 2019, julgada pelo juiz Guilherme Madeira Dezem, na qual devido a perseguição e *cyberstalking* por perfis falsos, foi feita a apelação para o Facebook, Microsoft, Google e TIM, com o objetivo de identificar o responsável e excluir os perfis, uma vez que o

apelante duvidava que fosse uma ex-namorada. Porém, devido as dificuldades de comprovação do ato, o provimento foi negado.

Em Apelação Cível nº 0003344-12.2015.8.26.0180, de 2019, julgado pelo relator J. B. Paula Lima, em que a apelante abriu ação contra o Facebook discorrendo sobre dano à imagem devido a circulação de vídeo pornográfico em grupos de WhatsApp, argumentando por passar a ser vítima de *cyberbullying*, estando também diretamente relacionada as questões impostas no Marco Civil da Internet.

Porém, no caso tratado, o Marco Civil da Internet ampara o provedor de internet sobre as responsabilidades causadas por terceiros, além de ser mencionada que a apelante não se tratava da autora do vídeo, o que não figura como prejuízo, e logo, teve o provimento negado pelo relator.

Dessa forma, observa-se em dois casos de *cyberbullying* onde foram necessários apelar o processo para as empresas com o objetivo de buscar a identificação ou remoção de conteúdo que estavam atingindo indiretamente. Mas em ambos os casos as provas foram insuficientes para prover recurso, podendo considerar o *cyberbullying* como um dos tipos mais difíceis de combate, sendo passível de tipos específicos de caso para o provimento de recurso.

4.3 PORNOGRAFIA INFANTIL

A pornografia infantil talvez seja o crime que gera maior repúdio na sociedade. Não há como aceitar a situação embaraçosa em que as crianças se encontram para interromper as fantasias de pessoas que estão fora de equilíbrio. A pedofilia é um fenômeno fora dos padrões comuns aceitos pela sociedade, e ela encontrou na Internet uma ferramenta que realmente satisfará os adeptos dessa prática.

Esta modalidade apareceu na Internet através das páginas anônimas que ficam na chamada *Deep Web*, que se trata dos sites que não são indexados com o nome padrão que se conhece, com os “.com”, “.org”, “.net”, dentre outros. Geralmente esses sites necessitam de cadastro, e para cadastrar solicitam uma quantia em dinheiro, paga com alguma criptomoeda, uma moeda virtual, para aumentar o anonimato.

A legislação brasileira se concentra primeiro na proteção de crianças expostas a crimes cibernéticos, principalmente sobre os métodos de mensagens de texto pornográficas. O artigo 241 do Estatuto da Criança e do Adolescente estipula que pessoas que possuem cenas

eróticas de menores de 18 anos serão sancionadas com 3 a 6 anos de reclusão (BRASIL, 1990).

Os pedófilos até criam dados pessoais falsos, fingindo ser crianças e trocando informações com menores para receber ligações de onde moram, depois iniciar conversas para ganhar confiança e até pedir fotos de nudez. Desta forma, esse fato se torna uma coisa normal que pode ser compartilhada e atrai a atenção das pessoas.

Os tribunais possuem diversos meios de lidar com o crime cibernético, mas ainda há lacunas, como vimos em todos os casos já citados. Os cidadãos ainda carecem de informação sobre essas questões, poucas pessoas estão cientes da possibilidade de trazer crimes virtuais para o judiciário e precisam tomar providências quando souberem como agir nessa questão.

E infelizmente, neste caso em especifico não foram mencionados casos da jurisprudência, porque em pesquisa no site JusBrasil, com o descritor de "Pornografia Infantil na Internet", apenas entre casos de 2015 para cima, a maioria se tratava de recursos de apelações e *habeas corpus*, na qual em leitura, a maioria estava sendo aceita para que esses criminosos respondessem o crime em liberdade.

Fica também uma crítica quanto a atualização das leis, pois no que tange a pedofilia e a pornografia infantil na internet, o Estatuto da Criança e do Adolescente ampara todas as situações que podem apresentar riscos as crianças e jovens, porém, um indivíduo que é culpado e depois ganha o dinheiro de responder em liberdade devido a recurso ou habeas corpus indica uma clara vulnerabilidade da lei, que é acatada pelo responsável pelo julgamento.

5 CONSIDERAÇÕES FINAIS

Este trabalho permitiu apresentar como a adaptação para leis voltadas a questões informáticas é complicada. O mundo da tecnologia envolve muitos obstáculos jurídicos e exige um processo profissional dos legisladores para adaptar e compreender o conteúdo relacionado às condições jurídicas específicas que precisam ser alteradas com mais rapidez.

Por mais difícil que pareça, o Direito precisa se adaptar, principalmente em relação ao amparo da população sobre os cibercrimes, porque o Brasil é um dos países que mais sofrem com esse tipo de situação, principalmente em relação aos crimes de estelionato ou golpes realizados pelo *phishing*.

A privacidade, o uso dos dados das pessoas nas redes, além dos diversos crimes já existentes e que encontraram brechas nas leis ao serem aplicadas por meios informáticos são algumas das questões que o Direito deve estar sempre levando em consideração na busca de melhorias jurídicas. Dessa forma, diversas leis puderam ser criadas, como a Lei Carolina Dieckmann, o Marco Civil da Internet e a atual Lei Geral de Proteção à Dados.

As três leis citadas são voltadas para questões informáticas, porém, somente a Lei Carolina Dieckmann possui características de combate a crime, enquanto as outras duas buscas a regularização e controle de como os dados dos usuários e a questão da privacidade é entendida pelas empresas.

Os outros crimes existentes, como estelionato, assédio moral, pedofilia, tiveram suas próprias leis adaptadas, sendo adicionadas em seus artigos a característica de crime também no uso de aparelhos informáticos. Isso não era o recomendado, uma vez que deveria ser feito um Código Penal voltado a crimes informáticos, com melhor tipificação de como o crime é realizado e penas de acordo com os impactos à vítima.

Porém, entende-se a dificuldade em criar uma nova regulação deste nível, adaptando as leis existente para possibilitar o setor judiciário em julgar e culpar quem são os envolvidos. Dessa forma, as leis voltadas para crimes informáticos realmente são eficientes para contribuir para o julgamento e amparar as vítimas.

Assim, para futuras pesquisas, este trabalho contribui com as principais questões históricas, doutrinárias e judiciais referente as leis voltadas para internet e cibercrime, sendo recomendado a pesquisa sobre quais outros crimes não citados neste trabalho ainda não possuem adaptação para realização na internet e seus impactos na população brasileira.

REFERÊNCIAS

ALEXANDRE JUNIOR, J. C. Cibercrime: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca**, v. 14, n. 1, 2019.

AZEREDO, J. S. **Território virtual e a face da violação do direito das mulheres**. 2020. 77f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Centro Universitário de Brasília, Brasília, 2020.

BRANDÃO, G.; GLASMEYER, R. **Golpe na Internet:** Como se proteger de estelionato virtual e o que fazer com a vítima de um crime digital. 2021. Disponível em: <>. Acesso em: 14.04.2021.

BRASIL. Lei nº 13.632 de 18/11/2010. Dispõe sobre a Política "Antibullying" nas instituições de ensino no município de Curitiba. **Diário Oficial Municipal**, Curitiba, 23 nov. 2010. Disponível em: <https://www.legisweb.com.br/legislacao/?id=174273>. Acesso em: 14.04.2021.

BRASIL. Superior Tribunal de Justiça. **Apelação cível nº 0003344-12.2015.8.26.0180, de 2019.** Disponível em: <https://tj-sp.jusbrasil.com.br/jurisprudencia/905036705/apelacao-civel-ac-33441220158260180-sp-0003344-1220158260180/inteiro-teor-905036999?ref=juris-tabs>. Acesso em: 10.07.2021.

BRASIL. Superior Tribunal de Justiça. **Apelação cível nº 0066760.87**. Disponível em: <https://tj-go.jusbrasil.com.br/jurisprudencia/771900789/apelacao-cpc-667608720168090051/inteiro-teor-771900802>. Acesso em: 10.07.2021.

BRASIL. Superior Tribunal de Justiça. **Apelação nº 1094247-20.2018.8.26.0100**. Disponível em: <https://tj-sp.jusbrasil.com.br/jurisprudencia/912666386/apelacao-civel-ac-10942472020188260100-sp-1094247-2020188260100/inteiro-teor-912666406>. Acesso em: 10.07.2021.

BRASIL. Decreto-lei no 2.848, de 7 de dezembro de 1940. Código penal. **Diário Oficial da União**, 7 dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 06.07.2021.

BRASIL. Lei nº 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. **Diário Oficial da União**, 29 out. 1984. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7232.htm>. Acesso em: 06.07.2021.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**, 05 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 05.06.2021.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, 13 jul. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 06.07.2021.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Diário Oficial da União**, 24 jul. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 06.07.2021.

BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. **Diário Oficial da União**, 19 fev. 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9609.htm>. Acesso em: 06.07.2021.

BRASIL. Lei no 9.983, de 14 de julho de 2000. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. **Diário Oficial da União**, 14 jul. 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9983.htm>. Acesso em: 06.07.2021.

BRASIL. Lei nº 11.829, de 25 de novembro de 2008. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. **Diário Oficial da União**, 25 nov. 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acesso em: 06.07.2021.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da União**, 30 nov. 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 06.07.2021.

BRASIL. 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**, 13 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 06.07.2021.

BRASIL. Lei nº 13.185, de 6 de novembro de 2015. Institui o Programa de Combate à Intimidação Sistemática (Bullying). **Diário Oficial da União**, 6 nov. 2015. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm>. Acesso em: 06.07.2021.

BRITO, W. L. **Os crimes virtuais na lei brasileira**. 2021. Disponível em: <https://conteudojuridico.com.br/consulta/artigos/56255/os-crimes-virtuais-na-lei-brasileira>. Acesso em: 06.07.2021.

CASTRO, B. B. Direito **Digital na Era da Internet Das Coisas – O Direito à Privacidade e o Sancionamento da Lei Geral de Proteção de Dados Pessoais**. 2019. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-civil/direito-digital-na-era-da-internet-das-coisas-o-direito-a-privacidade-e-o-sancionamento-da-lei-geral-de-protecao-de-dados-pessoais/>. Acesso em: 06.07.2021.

CAMARGO, G. C. **Vingança pornográfica**: contextualização do crime. 2020. 20 f. Trabalho de Conclusão de Curso (Bacharel em Direito) – UniCesumar – Centro Universitário de Maringá, Maringá. 2020.

CHAUVET, L. C. **Conceitos de crime**. 2016. Disponível em: <http://ambitojuridico.com.br/cadernos/direito-penal/conceitos-de-crime/>. Acesso em: 06.07.2021.

CNJ. **Crimes digitais:** quais são, quais leis os definem e como denunciar. 2018. Disponível em: <http://www.justificando.com/2018/06/25/crimes-digitais-quais-sao-quais-leis-os-definem-e-como-denunciar/>. Acesso em: 06.07.2021.

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

D'URSO, L. A. F. **Cibercrime:** perigo na internet! 2017. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/cibercrime-perigo-na-internet/ >. Acesso em: 16.06.2021.

DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**. 2. ed., São Paulo: Revista dos Tribunais, 2019.

FERNANDES, S. S. L.; CALDI, V. Do Reflexo do Desenvolvimento das Novas Tecnologias de Informação na Prática de Crimes contra Crianças e Adolescentes. In: SILVA, A. R. I. (Org.) **Crimes Cibernéticos**. Porto Alegre: Livraria do Advogado, 2017

G1. **Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera 'justiça'**. 2012. Disponível em: <http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>. Acesso em: 21.04.2021.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA – IBGE. **Pesquisa Nacional por Amostra de Domicílio**. 2018. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf>. Acesso em: 21.04.2021.

INSTITUTO DE REFERENCIA EM INTERNET E SOCIEDADE – IRIS. **O Brasil teve o maior vazamento de dados de sua história. E agora?** 2021. Disponível em: <https://irisbh.com.br/o-brasil-teve-o-maior-vazamento-de-dados-de-sua-historia-e-agora/>. Acesso em: 03.05.2021.

LAVADO, T. **Uso da internet no Brasil cresce, e 70% da população está conectada**. 2019. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/08/28/uso-da-internet-no-brasil-cresce-e-70percent-da-populacao-esta-conectada.ghtml>. Acesso em: 16.06.2021.

LEMOS, E. P. **Crimes virtuais:** a prática dos crimes cibernéticos. 2021. Disponível em: <https://www.conteudojuridico.com.br/consulta/Artigos/56376/crimes-virtuais-a-prtica-dos-crimes-cibernticos>. Acesso em: 16.06.2021.

LUCCHESI, Â. T.; HERNANDEZ, E. F. T. Crimes Virtuais: *ciberbullying*, *revenge porn*, *sextortion*, estupro virtual. **Revista Officium**: estudos de direito – v. 1, n. 1, 2018.

MARRA, F. B. Desafios do direito na era da internet: uma breve análise sobre os crimes cibernéticos. **Rev. Campo Jurídico, barreiras-BA**, v. 7, n. 2, p. 145-167, julho-dezembro, 2019.

MAUES, G. B. K.; DUARTE, K. C.; CARDOSO, W. R. S. Crimes virtuais: Uma análise sobre a adequação da legislação penal brasileira. **Revista Científica da FASETE**, v. 1, a. 2018. 2018.

MEDEIROS, M. **Como funciona a tramitação de um projeto de lei?** Disponível em: <https://exame.abril.com.br/blog/instituto-millenium/como-funciona-a-tramitacao-de-um-projeto-de-lei/>. Acesso em: 06.06.2021.

NASCIMENTO, K. **Instituto de Segurança Pública divulga dados de março**. 2020. Disponível em: <http://www.isp.rj.gov.br/Noticias.asp?ident=438>. Acesso em: 14 abr. 2021.

SANCHES, A. G.; ANGELO, A. E. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil**. Disponível em: <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil/2>. Acesso em: 06.06.2021.

SANTOS, P. E. B. Direito internacional e o combate à cibercriminalidade contra crianças. In: BRASIL. Ministério Público Federal. **Crimes cibernéticos**: crimes cibernéticos coletânea de artigos, volume 3. Brasília: MPF, 2018.

TOMASEVICIUS FILHO, E. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, n. 86. 2016.

VOINAROVSKI, I. M. L.; MAGALHAES, T. A. P. O tratamento do cybercrime no ordenamento jurídico brasileiro. **Revista Científica do Curso de Direito**, online, 2018 Disponível em: <https://www.fag.edu.br/upload/revista/direito/5db849cac6ef4.pdf>. Acesso em: 06.06.2021.