CENTRO DE EDUCAÇÃO SUPERIOR REINALDO RAMOS/CESREI

FACULDADE REINALDO RAMOS / FARR

CURSO DE BACHARELADO EM DIREITO

WALBER FERNANDES DANIEL

CRIMES DIGITAIS: COMO MELHORAR A EFETIVIDADE DAS SANÇÕES APLICADAS AOS INFRATORES.

Campina Grande

2021

WALBER FERNANDES DANIEL

CRIMES DIGITAIS: COMO MELHORAR A EFETIVIDADE DAS SANÇÕES APLICADAS AOS INFRATORES.

Trabalho Monográfico apresentado à Coordenação do Curso de Direito da Faculdade Reinaldo Ramos – FARR, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Prof. Diego Araújo Coutinho.

Campina Grande

2021

D184c Daniel, Walber Fernandes.
Crimes digitais: como melhorar a efetividade das sanções aplicadas aos infratores / Walber Fernandes Daniel. – Campina Grande, 2021.
44 f.

Monografia (Bacharelado em Direito) – Faculdade Reinaldo Ramos-FAAR, Centro de Educação Superior Reinaldo Ramos-CESREI, 2021.
"Orientação: Prof. Me. Diego Araújo Coutinho".

1. Crimes Digitais. 2. Redes Sociais – Crimes. 3. Internet. 4. Lei Geral de Proteção de Dados (LGPD). I. Coutinho, Diego Araújo. II. Título.

CDU 343.63:004.738.5(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

WALBER FERNANDES DANIEL

CRIMES DIGITAIS: COMO MELHORAR A EFETIVIDADE DAS SANÇÕES APLICADAS AOS INFRATORES.

Aprovada em: 14 de dezembro de 2021

BANCA EXAMINADORA

_____

Profe. Me. Diego Araújo Coutinho

Faculdade Reinaldo Ramos – FARR

(Orientador)

_____

Profe. Me. Rodrigo Araújo Reul

Faculdade Reinaldo Ramos – FARR

(1º Examinador)

_____

Profa. Ana Caroline Camara Bezerra

Faculdade Reinaldo Ramos – FARR

(2º Examinador)

Para

Meus pais (Valdegilton e Cláudia)

Minha esposa (Simone)

Minha filha (Lívia)

AGRADECIMENTOS

Agradeço à Deus pelo dom da vida e pelas oportunidades que me foi dada no decorrer dela.

Aos meus pais por sempre se esforçarem para fazer com que seus filhos tivessem toda a estrutura para percorrer o caminho do conhecimento.

A minha esposa por me apoiar durante toda a caminhada.

Ao meu sogro por se dispor a ajudar de diversas formas a trajetória das minhas conquistas.

RESUMO

A sociedade passa por um momento na história em que a tecnologia avança rapidamente e essa velocidade sempre tende a aumentar trazendo importantes benfeitorias ao mundo em diversos setores como na saúde, educação, lazer, economia e segurança. A criação da rede mundial de computadores foi um marco importante no que se refere a comunicação rápida entre locais remotos. Graças a ela as informações são passadas de um lado para outro do mundo em questões de segundos. Isso é de grande valia para o mundo globalizado em que vivemos pois qualquer acontecimento importante que ocorra em qualquer lugar do mundo será informado para todas as partes do planeta praticamente no mesmo instante em que ocorrera. Presenciamos efetivamente esta utilidade quando no fim do ano de 2019 u vírus desconhecido começou a infectar e matar pessoas em uma cidade na China. Em pouco tempo todo o mundo estava ciente da situação e com isso começaram a se preparar para receber possíveis infectados. Infelizmente não foi possível conter o vírus e a pandemia do novo coronavírus se instalou pelo mundo, mas é certo de que se não fosse a velocidade em que o mundo troca informações atualmente a situação da doença pelo mundo e o número de óbitos que ela trouxe seria muito pior do que já foi. Porem com todas as maravilhas que a evolução tecnológica trouxe, veio consigo delitos praticados via internet como invasão de equipamentos, vazamento de informações, furto de dados sigilosos, crimes contra a honra cometidos em redes sociais. E neste momento a solução encontrada foi a criação de leis para conter os crimes. No Brasil as principais leis que regulam a vida da sociedade no ambiente virtual são a Lei 12.965/14 conhecida como Lei Carolina Dieckmann, a lei 12965/14 conhecida como Marco Civil da Internet e a lei 13.709/18 conhecida como Lei Geral de Proteção de Dados. Portanto é de relevante valor fazer um estudo dessas leis e verificar as melhorias que possam a vir surgir para a solução desses delitos.

Palavras-chave: internet, redes, lgpd, crimes, digital.

ABSTRACT

Society is going through a moment in history when technology advances rapidly and this speed always tends to increase, bringing important improvements to the world in several sectors such as health, education, leisure, economy and security. The creation of the World Wide Web was an important milestone in terms of fast communication between remote locations. Thanks to it, information is passed around the world in a matter of seconds. This is of great value for the globalized world in which we live, as any important event that takes place anywhere in the world will be reported to all parts of the planet practically at the same moment it occurred. We actually witnessed this usefulness when, towards the end of the year 2019, an unknown virus began to infect and kill people in a city in China. Before long, the whole world was aware of the situation and with that they began to prepare themselves to receive possible infected people. Unfortunately it was not possible to contain the virus and the new coronavirus pandemic has set in around the world, but it is certain that if it were not for the speed at which the world currently exchanges information, the disease situation around the world and the number of deaths it brought would be much worse than it once was. However, with all the wonders that technological evolution has brought, crimes committed via the Internet have come with it, such as breaking into equipment, leaking information, stealing confidential data, crimes against honor committed on social networks. And at this moment, the solution found was the creation of laws to contain crimes. In Brazil, the main laws that regulate the life of society in the virtual environment are Law 12,965/14 known as the Carolina Dieckmann Law, the law 12965/14 known as the Marco Civil da Internet and the law 13,709/18 known as the General Law for the Protection of Data. Therefore, it is of relevant value to study these laws and verify the improvements that may arise for the solution of these crimes.

Keywords: internet, networks, lgpd, crimes, digital.

SUMÁRIO

INTRODUÇÃO

Este trabalho tem como objetivo obter informações que nos leve a entender a atual realidade dos crimes digitais no Brasil e de que forma eles são regulados pelo ordenamento jurídico pátrio.

Analisaremos a história da internet e do direito digital no mundo e especificamente no Brasil ressaltando sua importância para as sociedades. Passando pela evolução histórica do direito digital onde podemos ilustrar a caminhada da tecnologia pelas sociedades focando no século XX, considerado o mais importante para o desenvolvimento da tecnologia que se materializou na criação do telefone, da TV e dos primeiros passos da Internet. Abordaremos os primórdios da Internet no Brasil, mostrando sua evolução e como o país se preparou para receber a infraestrutura da rede.

Conceituaremos o Direito Digital mostrando a importância e a evolução deste instituto para o ordenamento jurídico mundial e especificamente para o Brasil. Abordaremos a relação que este ramo do direito tem com os ramos tradicionais da ciência jurídica mostrando a ajuda que o direito digital trouxe para os ramos tradicionais do direito como a utilização dos institutos tradicionais do direito na formação legal do direito digital.

O presente trabalho também abordará a legislação nacional explanando as noções gerais sobre o tema e trazendo informações importantes sobre as principais leis que regem o direito digital atualmente no Brasil como também os principais crimes cometidos em meio digital no país, o perfil dos criminosos e as dificuldades encontradas para investigar os delitos.

Discutiremos o tema utilizando alguns autores como, Patricia Peck, Damásio de Jesus, Marcelo Crespo dentre outros. A metodologia utilizada terá cunho interdisciplinar usando estudo de pesquisa qualitativa e bibliográfica para chegar ao resultado desejado.

Algumas considerações foram realizadas a respeito das sanções aplicadas aos infratores de crimes digitais e analisamos como o ordenamento jurídico

brasileiro e a própria sociedade se comporta neste aspecto mostrando caminhos que levem a uma melhor efetividade nestas punições.

1 EVOLUÇÃO HISTÓRICA DO DIREITO DIGITAL

Quando falamos em direito digital, estamos falando simplesmente na evolução do direito tradicional, visando aprimorar a aplicabilidade dos princípios fundamentais e institutos na esfera jurídica como também introduzir novas vertentes ao pensamento jurídico atual nas mais diversas áreas do direito. Mas para isso, a sociedade percorreu um longo período até que conseguíssemos chegar à realidade atual. Há pouco tempo, a internet não passava de um projeto que visava romper fronteiras na disseminação de informações computacionais e quando esse objetivo foi atingido no início, a tecnologia era restrita à algumas universidades e órgãos de governos de países desenvolvidos, estritamente limitado e de alto custo. No mundo jurídico as coisas ocorriam resumidas a papéis, burocracia e prazos.

Antes dos século XX, se comunicar era uma tarefa complicada e demorada, através da tradicional carta, considerada o meio de comunicação mais antigo do mundo, e foi através dela que os colonizadores portugueses conseguiram informar à Corte Portuguesa a descoberta do “novo mundo” nos tempos do descobrimento do Brasil. Depois da carta e a passos lentos, a comunicação foi evoluindo coma chegada do serviço de envio de documentos mediante pagamento como os correios, depois veio o telégrafo e no século XIII, com o boom ocasionado pela revolução industrial e com isso o aprimoramento da ciência e tecnologia da época, surge o meio de comunicação que alterou radicalmente o modo de se comunicar entre as pessoas, o telefone. Em 1876, a criação de Graham Bell possibilitou o diálogo e a rapidez entre dois pontos distantes. Não podemos deixar de destacar o rádio e sua importância para a comunicação em massa do século XIX e XX com destaque para a sua intensa utilização durante as duas grandes guerras mundiais. Após o rádio, tivemos a chegada da televisão e com isso a informação deixa de ser apenas ouvida e passa a ser vista, tornando a TV o meio de comunicação em massa mais acessível do séc. XX.

Após a evolução da comunicação trazida pela TV, o mundo estacionou por um período e só voltou a revolucionar o modo de se comunicar com a popularização da internet. A história da Internet começa a ser contada no período de tensão da guerra fria que ocorrera de 1945 a 1991. Estados Unidos e União Soviética

disputando hegemonia e supremacia do capitalismo e socialismo travavam essa guerra silenciosa e tensa. Com o intuito de facilitar a troca de informações temendo possíveis ataques soviéticos foi desenvolvido um sistema de troca de informações a longas distâncias para melhorar as estratégias de possíveis ataques e consequentemente a defesa. Esse sistema foi desenvolvido peça Agência de Projetos de Pesquisa Avançada (*Advanced Reseach Projects Agency*) ou simplesmente ARPA. E em 29 de outubro de 1969 a ARPANET estabeleceu a conexão entre a universidade da Califórnia e o Instituto de Pesquisa de Stanford.

A aparição da internet no Brasil se deu nos anos 80 quando universidades brasileiras começaram a trocar informações com os Estados Unidos. No fim dos anos 80 foi fundado aqui no Brasil a Rede Nacional de Ensino e Pesquisa (RNP) com o objetivo de disseminar a tecnologia da internet no país e facilitar a troca de informações e pesquisas. Neste período foi criado um servidor *backbone* conhecido como *Backbone* RNP. Servidor *backbone* é o servidor responsável por integrar servidores distantes entre si, é conhecido como a espinha dorsal da internet. Este *backbone* integrava 11 estados brasileiros através de suas capitais. A partir deste período a internet no Brasil não parou de evoluir e em 1998 o país já era o 19ª em número de *hosts* (hospedagens) no mundo e dentro do continente americano, ficava atrás apenas dos Estados Unidos e Canadá.

A internet passou a ser fundamental a vida das pessoas e das empresas que começaram um processo ambicioso de digitalização e muitos armários de documentos foram ganhando formas digitais e armazenados em HDs, disquetes, CDs DVDs até chegarmos aos dias atuais com o armazenamento em nuvem. Com esse avanço, não restou opção ao Direito que teve que acompanhar as mudanças que a sociedade vinha promovendo, adequando seus institutos e criando novos a fim de regular os acontecimentos neste meio, haja vista que o avança tecnológico traz mudanças significativas nas relações jurídicas e faz com que os operadores do direito vivem em constante atualização.

1.1 Conceito e aplicabilidade

Podemos considerar o Direito Digital como sendo a evolução do Direito. E esta evolução faz com que o Direito se integre às mudanças que a sociedade atual trouxe consigo. É a integração dos institutos tradicionais do Direito aos *softwares*,

redes e todo o tipo de ação e omissão perpetrados pela sociedade utilizando de meios digitais para tais condutas.

“O direito é a evolução do próprio direito de uma sociedade digital. Para isto, a tecnologia vem contribuindo desde 1920, com a expansão dos veículos de massa e mais recente com o telefone celular, o e-mail, a internet, a banda larga, a TV Interativa” (PECK, 2009. P21)

Direito digital ou direito informático é o conjunto de normas e instituições jurídicas que pretendem regular aquele uso dos sistemas de computador – como meio e como fim – que podem iniciar nos bens jurídicos dos membros da sociedade, as relações derivadas da criação, uso, modificação, alteração e reprodução do software, o comércio eletrônico e as relações humanas estabelecidas via internet. (PAIVA, 2019).

Como podemos observar, o direito digital nasce como uma atualização do direito com o objetivo de regular as relações jurídicas em meio digital. Agora temos o comércio eletrônico que não deixa de ser uma relação jurídica de consumo, regulada pelo Código de Defesa do Consumidor, porém nem sempre seria viável e justo utilizar-se das normas previstas neste código que regulam as práticas consumeristas em meio físico e tradicional para aplicá-las em meio virtual considerando algumas peculiaridades que encontramos no comércio eletrônico, o consumidor poderia sair abusado de uma relação de consumo em meio digital. Tomando como exemplo a compra de um produto em meio físico: o CDC não exige que o estabelecimento comercial receba de volta o produto adquirido pelo simples fato do consumidor não ter gostado ou por ter se arrependido da compra, alguns estabelecimentos podem receber, trocar por outro produto mas por livre e espontânea vontade, pois a legislação não exige tal conduta, agora se esta compra for realizada em meio não presencial, ou seja, por telefone, internet, app, o CDC garante ao consumidor o direito de arrependimento da compra em um prazo de 7 dias após recebido o produto. É o que diz o Art. 49 caput e seu Parágrafo único do Código de Defesa do Consumidor:

> “Art. 49. O consumidor pode desistir do contrato, no prazo de 7 dias a contar de sua assinatura ou do ato de recebimento do produto ou serviço, sempre que a contratação de fornecimento de produtos e

> serviços ocorrer fora do estabelecimento comercial, especialmente por telefone ou em domicílio.
>
> Parágrafo único. Se o consumidor exercitar o direito de arrependimento previsto neste artigo, os valores eventualmente pagos, a qualquer título, durante o prazo de reflexão, serão devolvidos, de imediato, monetariamente atualizados.”

Este Artigo é importante para equacionar a relação de consumo virtual da presencial haja vista que numa compra virtual o consumidor tem como referência do produto apenas imagens, vídeos que podem não retratar fielmente o produto real e por este motivo se dar o direito de arrependimento. Podemos citar também os fatos que ocorrem rotineiramente nas redes sociais e os cuidados com as informações disseminadas nelas onde o direito está em evolução buscando combater a violação de informações pessoais, imagem, privacidade dentre outros bens.

> Nos encontramos em uma situação de transição, de mutação do Direito, em que a falta de adequação dos processos jurídicos e dos seus profissionais gera ainda mais incerteza, insegurança quanto a capacidade de vivermos em um estado de legalidade. É por isso, que surge o Direito Digital, com uma abordagem mais estratégica e uma visão mais ampla do Direito com respostas para as questões atuais que mais têm gerado polêmica e que são fruto da nova realidade social, como a Privacidade, Segurança, Consumidores Virtuais, e-Commerce, E-mail, Exclusão Digital, Governo Eletrônico, Crimes de Internet, Empresa Virtual, Acesso Banda Larga sem necessidade de Provedor, Legitimidade dos Disclaimers, Substituição de leis por softwares que regulam condutas e comportamentos na rede, Importação de bens não materiais via Internet, Publicidade Online e o Código do Consumidor, Uso de Banco de Dados. Vamos apresentar sempre um tema que traz problema e solução jurídica mais adequada, com embasamento legal atual. Vamos ver que no Direito Digital o que vale é a melhor estratégia. A complexidade da sociedade atual traz uma maior complexidade jurídica, e faz, cada vez mais, que o advogado tenha que ser um estrategista. Não é mais suficiente conhecer apenas as Leis; devem-se conhecer os modelos que conduzem o mundo das relações entre pessoas, empresas, mercados, Estados. Cabe ao profissional de Direito dar os caminhos e as soluções viáveis, pensadas no contexto competitivo e globalizado de um possível cliente virtual-real, convergente e multicultural. (PECK, 2019).

Como já podemos observar, o ramo do Direito Digital é bastante amplo podendo fazer o profissional que queira atuar nesta área atuar no contencioso, consultivo, *compliance*, contrato e atrelado ao direito penal.

No contencioso, o profissional da área irá trabalhar casos envolvendo violações de informações pessoais, prática bastante comum atualmente e que trazem bastante desconforto às vítimas gerando consequências consideráveis, tanto que os órgãos superiores do judiciário já vêm entendendo que tais condutas geram pagamentos de danos materiais, morais com o intuito de diminuir e ressarcir os impactos dessas exposições nas vítimas. Além das questões cíveis, o profissional poderá encontrar litígios trabalhistas, tributários, previdenciários e de proteção dos direitos autorais atrelados ao direito digital.

Na maioria dos casos o Direito Digital não chega trazendo matérias inéditas, acontece apenas a mudança na interpretação da legislação vigente fazendo com que os operadores do direito se esforcem para a trazer a analogia das normas vigentes aos fatos.

Atuando em meio consultivo o profissional poderá se relacionar com empresas que atuam em meios misto (físico e digital) e com as empresas que atuam exclusivamente em meio digital. As lojas virtuais ou e-commerces atuam oferecendo produtos e serviços por meio de sites e perfis de redes sociais e estas ações por muitas vezes enchem de dúvidas os empreendedores do meio, que necessitam de consultoria especializada para atuar se ferir o CDC e o Código Civil.

O que mais empurrou o direito digital no caminho da evolução foram os crimes praticados na internet, os crimes digitais. A sociedade tinha a ideia de que internet ou mundo virtual seria uma terra sem lei, um mundo sem dono onde tudo pode e tudo acontece e o que lá se fazia não trazia consequências jurídicas para o agente no mundo físico. Este pensamento vem mudando com o tempo e com a evolução do combate aos delitos praticados online, porém ainda com uma grande ineficácia em punir corretamente estes infratores.

O crime digital, assim como o crime em meio real, nada mais é do que uma conduta típica, antijurídica e culpável e o que difere o crime digital do crime em meio físico são as ferramentas utilizadas para cometer o ato ilícito. Podemos dizer que os principais crimes praticados na internet são: o furto de informações pessoais, os crimes contra a honra (calúnia, injúria e difamação), e os crimes contra os consumidores.

> O crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual; contudo, em certos casos, o crime não. A maioria dos crimes cometidos na rede ocorre também no mundo real. A Internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória, bem como à necessidade de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio. Os crimes eletrônicos ou cibernéticos têm modalidades distintas, dependendo do bem jurídico tutelado. Nesse sentido, podemos dar como exemplo o crime de interceptação telefônica e de dados, que tem como bem jurídico tutelado os dados, ou seja, o que se quer é proteger a transmissão de dados e coibir o uso dessas informações para fins delituosos, como, por exemplo, captura de informações para envio de “e-mail bombing”, o “e-mail com vírus”, o “spam”. Esse tipo penal protege também a questão da inviolabilidade das correspondências eletrônicas. (PECK, 2013).

1.2 Direito digital e outros ramos

Mesmo deixando a entender que existam dois universos paralelos quais sejam, o real e o virtual, não devemos levar como verdadeira essa informação. O que devemos entender é que existe um universo virtual inserido em nosso mundo real e por isso requer atenção do Direito pois este universo traz consigo situações e consequências que já fazem parte do cotidiano da sociedade causando impactos e requerendo seriedade na gerência destes.

De certo modo, o Direito Digital possui autonomia, mas nada obsta que este ramo do Direito estabeleça conexões com outros pois tudo é direito e estes ramos de alguma forma convergem em busca da justiça.

Considerando o Direito Constitucional, o ramo do direito que estuda e engloba a lei suprema de um Estado, iniciamos com a relação do Direito Digital com o Direito Constitucional. A relação pode ser considerada vasta visto que a constituição por ser a lei suprema e mesmo sem encontrarmos dispositivos específica para abraçar o Direito Digital na carta, podemos usar os princípios e garantias presentes nesta e atrelá-los aos fatos que porventura ocorram em meio digital.

A constituição de 1988 mesmo sem mencionar o Direito Digital garante, mesmo que por meio eletrônico, a liberdade, a propriedade e o sigilo da correspondência, quando estabelece em seu Artigo 5º caput:

> “Todos são iguais perante a lei sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e a propriedade, nos seguintes termos.” “XII – é inviolável o sigilo da correspondência...”.

A nossa constituição nos garante respeito a vida privada, à intimidade, nos garante o sigilo da correspondência, correspondência esta que por analogia citamos as mensagens trocadas por e-mail, SMS, aplicativos de mensagens instantâneas como o *WhatsApp* sem que ninguém possa interferir com a intenção de saber do que se trata o conteúdo, haja vista se tratar de informações de caráter privado que só diz respeito a quem enviou e recebeu e essa inviolabilidade só poderá ser quebrada por decisão judicial com fundamento que mostre interesse público na causa.

Portanto, partindo do pressuposto que a Constituição de um Estado é a lei das leis, e que o Direito Digital por ela está abraçado, podemos considerar mais uma vez que o Direito Digital tem relação com todos os outros ramos do direito por trazer poucos novos institutos e muito mais atualizações e adequações dos que já existem para que sejam úteis em um ambiente digital.

2 CRIMES DIGITAIS E A LEGISLAÇÃO NACIONAL

Os crimes digitais, também denominado crimes cibernéticos ou virtuais crescem na sociedade na mesma velocidade em que a internet domina nosso cotidiano e este crescimento preocupa a sociedade porque com ele cresce também o número de infrações cometidas por este meio fazendo com que muitos desses delitos fiquem impunes por falta ou deficiência de legislação específica, forçando o Estado a se movimentar e adequar a legislação nacional aos novos delitos provenientes deste novo meio de interação da sociedade.

2.1 Noções gerais

Para falarmos a respeito dos crimes digitais é benéfico uma volta no tempo para compreender melhor a evolução histórica destes atos. A sabotagem em máquinas é datada de 1820 quando funcionários se sentindo ameaçados peala invenção criada pelo seu patrão, a máquina de tear, sabotaram-na para desencorajar o inventor e com isso manter seus empregos haja vista, a máquina de tear criada por Joseph-Marie Jacquard possibilitava a produção em grande escala comparado ao trabalho humano da época. Seguindo esse pensamento podemos citar o trabalho de Alan Turing, recrutado pela CIA (Agência de Inteligência Americana) para decifrar as mensagens codificadas alemãs e com isso fazer o país se antecipar em possíveis ataques e defesas.

Existem divergências doutrinárias em relação ao ponto específico que caracteriza o primeiro crime digital cometido no mundo. Algumas correntes de pesquisa acreditam ter ocorrido o primeiro crime digital em 1964, outras ter ocorrido em 1978, mas independentemente dessas duas datas podemos destacar que neste período ainda não existia lei sobre crimes digitais e que a partir de 1978 foi formulada nos Estados Unidos mais precisamente no Estado da Flórida, as primeiras codificações legais sobre informática.

No continente europeu em 1976 foi realizada a Conferência Sobre Aspectos Criminológicos do Crime Econômico e este debate é considerado como sendo a primeira manifestação internacional com a finalidade de debater e compreender os aspectos legais dos crimes digitais.

> Entretanto, foi nas décadas de 1980 e 1990 que grande parte dos cibercrimes se propagou. Já na década de 1980, John Draper (Capitain Crunch), conhecido por ser o inventor do phreaking, usou um apito para produzir o tom de 2.600 Hz, capaz de enganar o sistema telefônico americano. Deste modo, conseguia realizar ligações gratuitamente. (JESUS, 2016, p.26)

Nas décadas de 80 e 90 os criminosos já tinham suas condutas preferidas em meio eletrônico, foi nesse período que se propagaram a disseminação de vírus, pornografia infantil, invasão de sistemas e pirataria e daí inicia-se em contrapartida a preocupação dos Estados com a segurança dos sistemas. Em 1990 o mundo já conhecia termos como *NetWar* (Guerra de Informação) e o *Hacktivists* que segundo o site Wikipedia.org, significa: Hacktivismo (uma junção de hack e activismo) é normalmente entendido como escrever código fonte, ou até mesmo manipular bits, para promover ideologia política - promovendo expressão política, liberdade de expressão, direitos humanos, ou informação ética. Atos de hacktivismo são carregados da crença de que o uso de código terá efeitos similares aos do ativismo comum ou manifestações civis. Poucas pessoas podem escrever código, mas o código afeta muitas pessoas.

> Robert Morris foi o responsável por criar um dos primeiros vírus de computador no mundo, que prejudicou 6 mil computadores em 1988. Foi também o primeiro hacker a ser condenado pela então nova Computer Fraud Act norte-americana. Em 1990, Kevin Mitnick invadiu a rede de computadores das operadoras de telefonia e provedores de Internet dos Estados Unidos. Foi preso em 1995 e ficou cinco anos detido. Ainda em 1990, Kevin Poulsen interceptou as ligações a uma emissora de rádio na Califórnia e por ser o 102º ouvinte, ganhou um Porsche. Foi preso por quatro anos e hoje é diretor do site Security Focus. Nunca mais paramos de conhecer novos casos de hacking no mundo. (JESUS, 2016, p.27)

No Brasil os crimes digitais passaram a fazer parte da pauta de preocupações das autoridades há cerca de duas décadas. Atualmente o país é considerado o quinto do mundo em alvos de crimes digitais e neste ano de 2021 já houve mais ataques cibernéticos no Brasil do que em todo o ano de 2020. Isto é um dado muito expressivo visto que as maiores mudanças nos comportamentos da sociedade em razão da pandemia do coronavírus (COVID-19) ocorreu justamente no ano de 2020 e com os decretos e restrições de locomoção veio a alta demanda pelos serviços digitais utilizando computadores, smartphones e TVs para trabalho, estudo e lazer e com a alta demanda desses serviços cresce também o número de vítimas de crimes

digitais e mesmo com todo esse crescimento de utilização dos meios digitais no ano mais recluso da sociedade dos últimos tempos, o primeiro semestre de 2021 consegue bater a quantidade de ataques virtuais de todo o ano anterior. O Brasil é considerado o berçário dos criminosos virtuais pois abriga 80% dos hackers do mundo, dois terços dos responsáveis por crime de pedofilia praticados na internet no Brasil e no exterior tem origem brasileira.

A internet permite que criminosos tenham em suas mãos uma considerada quantidade de pessoas vulneráveis aos seus crimes e golpes e isso pode ser uma das razões que explica a derrocada de infrações por meio digital que o mundo vem passando. Com uma simples alteração em uma linha de comando de um software, um hacker consegue furtar dados, desestruturar sistemas, furtar bens de valores, um pedófilo com uma única imagem consegue dizimar seu ato criminoso por todo o planeta em questão de segundos e tudo isso utilizando-se da falsa sensação de impunidade, anonimato e terra sem lei que muitos ainda ousam acreditar que é a rede mundial.

De acordo com a Central Nacional de Denúncias de Crime Cibernético, em 2020 foram registradas 156.692 denúncias anônimas relacionadas a crimes digitais dentre os quais estão listados a fraude por *email* ou internet, a fraude de identidade, que ocorre quando os dados pessoais das vítimas são roubados e utilizados para fins diversos trazendo prejuízo moral e material aos lesados, o roubo de dados financeiros, que geralmente estão relacionados aos dados de acesso aos aplicativos de celular e dados de cartões de crédito, o roubo e venda de dados corporativos, que ocorre quando empresas contratam criminosos para roubar informações sigilosas de outras empresas concorrentes para que com o ato ilícito se beneficie em futuros acordos e ações de crescimento comercial, extorsão cibernética por *Ransonware*, que exige dinheiro para impedir o ataque ou decodificar os arquivos alterados, com o crescimento do mercado de criptomoedas cresceu junto o crime de *cryptojacking* que ocorre quando hackers exploram criptomoedas usando recursos que não possuem.

Fica concluso no parágrafo anterior que muitas condutas criminosas em meio digital requerem vasto conhecimento técnico na área computacional para que os efeitos do delito sejam atingidos, porém as novas ferramentas digitais podem ser apenas utilizadas em seu manuseio básico para o cometimento de outros crimes e

com isso exigir menos técnica computacional. É o que ocorre por exemplo nos crimes contra a honra praticados em uma rede social. Para a prática deste crime em meio virtual basta o autor do delito ter o básico de conhecimento de uso da ferramenta de interação social, realizar comentários ofensivos em relação a vítima e que não condizem com a verdade para que a vítima se insurja e busque os meios judiciais para informar sobre o crime que fora cometido em seu desfavor.

2.2 Classificação dos crimes digitais

Para classificar os crimes digitais precisamos compreender que o direito penal já está entrelaçado aos meios informáticos formando um complexo de normas e regulamentos jurídicos com a finalidade de coibir delitos.

Existem diversos posicionamentos doutrinários em relação à classificação dos crimes digitais e dentre os principais podemos citar o posicionamento de Klaus Tiedemann, jurídico alemão que na década de 80 classificou os crimes digitais os quais ele chamava de “criminalidade informática” em: manipulações, espionagem, sabotagem e furto de tempo.

Onde a manipulação seria afetar o processamento de dados do sistema computacional; a espionagem como subtração de informações confidenciais armazenadas nos sistemas; sabotagem como a destruição dos sistemas e a utilização de forma errada dos sistemas por empregados desleais ou estranhos para o furto de tempo.

> Martine Briat (1985, p. 287), autora francesa, buscou classificar os delitos informáticos em crimes onde a informática é o meio para a prática delituosa, e os demais delitos, onde, nesta categoria, citamos:
>
> a) manipulação de dados e/ou programas a fim de cometer uma infração já prevista pelas incriminações tradicionais;
> b) falsificação de dados de programas;
> c) deterioração de dados e de programas e entrave à sua utilização;
> d) divulgação, utilização ou reprodução ilícita de dados e de programas;
> e) uso não autorizado de sistemas de informática; e
> f) acesso não autorizado a sistemas de informática. (JESUS, 2016, p.84)

> "Rovira del Canto (2002, p.128), por sua vez, tem uma das classificações mais amplas sobre delitos informáticos, sendo elas:
> a) infrações à intimidade;
> b) ilícitos econômicos;

> c) ilícitos de comunicação ou difusão de conteúdos ilegais ou perigosos;
> d) outros delitos." (JESUS, 2016, p.85)
> "Ulrich Sieber (2008, apud CRESPO, 2011, p. 60) emitiu parecer para a Comissão Europeia sobre crimes informáticos, classificando-os em:
> a) violação à privacidade;
> b) crimes econômicos:
> b.1) hacking;
> b.2) espionagem;
> b.3) pirataria em geral (cópias não autorizadas);
> b.4) sabotagem e extorsão;
> b.5) fraude;
> c) conteúdos ilegais e nocivos;
> d) outros ilícitos;
> d.1) contra a vida;
> d.2) crime organizado;
> d.3) guerra eletrônica." (JESUS, 2016, p.83)

Analisando o posicionamento dos doutrinadores temos como base a linha de pensamento da classificação dada por Martine Briat (1985) e da classificação dada por Damásio de Jesus (2016) que sustentam a tese de que a informática é apenas meio utilizado por criminosos para o cometimento de crimes já tipificado no código, bens jurídicos tutelados pelo código penal, mas também os crimes de pura informática que são os de violação de sistema e dados que são os bens jurídicos propriamente ditos.

Portanto, classificamos os crimes digitais em crimes digitais próprios que são os crimes que o bem jurídico é a tecnologia computacional propriamente dita. Este tipo de crime passou algum tempo carente de legislação específica e a justiça nada poderia fazer para punir os infratores pois estes estavam sentados sobre o princípio da reserva legal do direito penal e suas infrações não poderiam ser enquadradas como crimes; Crimes digitais impróprios que são aqueles delitos que apenas usam a tecnologia da informação como ferramenta para atingir bens jurídicos já tutelados pela legislação pátria e tipificados no Código Penal brasileiro; Crimes digitais mistos que caracterizam-se pela junção do crime próprio com o impróprio e nessa situação além de violar o bem jurídico informático, violam bem jurídico distinto já tipificado em lei; Crime digital mediato ou indireto que trata-se da infração digital realizada com a finalidade de cometer outro delito que não será de ordem digital. Podemos dar como exemplo de crime digital indireto a situação em que o agente intercepta dados do cartão de crédito da vítima e realiza compras em seu favor caracterizando assim apenas o crime-fim de furto.

Damásio de Jesus (2016) assim classifica os crimes digitais:

> a) crimes informáticos próprios: em que o bem jurídico ofendido é a tecnologia da informação em si. Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente;
>
> b) crimes informáticos impróprios: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais;
>
> c) crimes informáticos mistos: são crimes complexos em que, além da proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico;
>
> "d) crime informático mediato ou indireto: trata-se do delito informático praticado para a ocorrência de um delito não informático consumado ao final. Em Direito Informático, comumente um delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial. Como, por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consunção, o agente só será punido pelo delito-fim (furto)." (JESUS, 2016, p.86)
>
> A simples utilização de um computador para a perpetração de um delito como um estelionato não deveria ser – repita-se – com precisão técnica, considerada um crime informático. Ocorre, todavia, que não só autores, mas também as mídias em geral, convencionaram denominar crimes informáticos qualquer delito praticado com o uso da tecnologia, seja ela o instrumento da conduta, seja o objeto do ilícito. Destarte, apesar de não ser a mais técnica, a nosso ver, é impossível ignorá-la, dada sua particular popularidade acadêmica e, por que não, social, vez que mesmo a mídia em geral passou a se valer dessa mesma classificação (CRESPO, 2011, p.63)

2.3 Procedimento para realização de requerimento ou queixa-crime.

Como já explanado no capítulo anterior, a sociedade ainda insiste em achar que o mundo virtual é uma terra sem lei, onde o anonimato reina soberano, mas podemos afirmar que a cada dia que passa o anonimato virtual perde força e atualmente é muito mais dificultoso a ocultação pessoal em ambiente virtual. Com o avanço tecnológico atualmente é possível rastrear infratores e procurar responsabilizá-los civil e penalmente se vierem a cometer atitudes em desconformidade com a legislação pátria. Não deixando no esquecimento àqueles que mesmo não sendo portadores de habitualidade delitiva acabam praticando

comportamentos excessivos que de alguma forma atinge outras pessoas ou cause repúdio na sociedade por tais atos.

Na esfera penal os crimes digitais mais comuns são aqueles que ferem a honra de alguém. Os crimes contra a honra têm previsão legal em nosso código penal mais precisamente nos artigos 138, 139 e 140 tipificando respectivamente os crimes de calúnia, difamação e injúria.

Cada um desses delitos possui requisitos próprios e além de tipificados no código penal também estão previstos em legislações especiais como o Código Eleitoral e o Código Militar. Para melhor compreensão cabe fazer a distinção destes três crimes para facilitar a identificação do delito cometido em um caso concreto e associá-lo corretamente ao tipo penal.

Calúnia.

Art. 138. Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena — detenção, de seis meses a dois anos, e multa.

§ 1º Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.

> Na calúnia o agente faz uma imputação de fato criminoso a outra pessoa, ou seja, ele narra que alguém teria cometido um crime. Como a calúnia dirige-se à honra objetiva, é necessário que essa narrativa seja feita a terceiros e não ao próprio ofendido. Não basta, ademais, que o agente chame outra pessoa de assassino, ladrão, estelionatário, pedófilo, corrupto etc., porque, em todos esses casos, o agente não narrou um fato, mas apenas xingou outra pessoa. (GONÇALVES, 2011, P.235)

Dentre os 3 crimes que aqui explanaremos o crime de Calúnia é o mais grave pois nele o agente conta uma história falsa em que nela a vítima comete um crime ferindo assim sua honra objetiva e para que a calúnia se configure precisa ser a história transmitida à terceiros e não a própria vítima além do mais não basta apenas imputar crimes à vítima como por exemplo chama-la de ladrão, bandido, para se configurar o crime de calúnia o agente precisa narrar uma história em que dentro desta a vítima teria cometido um crime.

Difamação

Art. 139. Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena — detenção, de três meses a um ano, e multa.

> Conforme indica o próprio nome do delito, difamar significa causar má fama, arranhar o conceito de que a vítima goza perante seus pares, abalar sua reputação. Tal como ocorre na calúnia, a difamação pressupõe que o agente atribua à vítima um fato determinado, concreto, que, aos olhos de outrem, seja algo negativo. (GONÇALVES, 2011, P.244).

O crime de difamação consiste em manchar de alguma forma a imagem que a vítima tem perante a sociedade. Diferentemente da Calúnia que para se caracterizar o agente precisa narrar um fato delitivo em que a vítima seria a criminosa, na Difamação o leque é mais abrangente podendo o agente utilizar-se de qualquer menção, nomenclatura, palavra que venha a ferir a imagem pessoal da vítima na sociedade como por exemplo que o pintor foi trabalhar embriagado e fez um péssimo serviço, que uma mulher entrou em um carro para fazer programas sexuais, que o marido tem relações extraconjugais com a vizinha. E ao contrário da Calúnia, na Difamação a lei não exige que a imputação seja falsa, para caracterizar o crime de Calúnia a imputação do fato precisa ser falso, na Difamação mesmo sendo verdadeiro o fato, nada obsta que a vítima, se sentindo atingida, procure reparação judicial. A lei neste caso mostra que cada pessoa deve tomar conta de sua vida e deixar de lado o que ocorre na vida alheia e caso isso não ocorra, mesmo o fato divulgado sendo verdadeiro poderá responder criminalmente por de alguma forma se intrometer na vida alheia.

Injúria

“Art. 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena — detenção, de um a seis meses.”

> A injúria difere totalmente dos outros crimes contra a honra porque é o único deles em que o agente não atribui um fato determinado ao ofendido. Na injúria, o agente não faz uma narrativa, mas atribui uma qualidade negativa a outrem. Consiste, portanto, em um xingamento, no uso de expressão desairosa ou insultuosa para se referir a alguém. A característica negativa atribuída a alguém, para configurar injúria, deve ser ofensiva à sua dignidade ou decoro. (GONÇALVES, 2011, P.249).

A Injúria ataca os atributos morais da vítima, dizendo por exemplo que alguém é safado, velhaco, piranha, vagabunda, prostituta. No que tange a ofensa ao decoro,

ataca os atributos físicos e intelectuais da vítima como por exemplo atacá-la chamando-a de burro, gorducha, idiota, imbecil, fedorento.

Os crimes contra a honra são disparados os mais comuns praticados em meio virtual, mas existe vários outros delitos que são praticados diariamente na sociedade atual:

Estelionato

“Art. 171, caput — 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.”

O estelionato é um crime contra o patrimônio muito comum de ser praticado nas redes sociais e site de compra e venda. É um crime marcado pelo emprego de fraude, que o agente utilizando de alguma manobra, artimanha engana a vítima fazendo com que esta se sinta segura o suficiente para entregar algum bem ao agente que com isso usa este bem em seu favor ou de terceiros.

Os sites de compra e venda de produtos seminovos é um atrativo para criminosos que praticam estelionato. O site OLX por exemplo é um dos mais populares entre os vendedores e compradores de automóveis e muito utilizado pelos golpistas. Um dos golpes mais conhecidos deste site é o que um estelionatário duplica o anúncio de venda de um automóvel com um valor mais baixo do que o original, algumas pessoas são atraídas pelo valor mais baixo do veículo, iniciam a negociação, transfere quantias na esperança de segurar a venda e depois de efetuado a transferência o agente desativa o anúncio.

> Golpe do falso intermediário é um dos mais usados no mercado de compra e venda de carros usados. Ação consiste no criminoso enganar duas pessoas com um argumento diferente para cada vítima, sem que uma converse com a outra sobre o meio de pagamento e o valor a ser tratado. (FANTÁSTICO, 2021)

É importante frisar que além destes crimes listados acima muitos outros, inclusive mais gravosos são praticados diariamente em meio digital como o crime de ameaça, violação de sistemas de segurança, apologia ao crime, estupro virtual,

pornografia infantil, violação da liberdade religiosa, racismo, crime de ódio, todos praticados por pessoas que utilizam a rede para consumar tais delitos.

O que não se discute é que estas atitudes cometidas na internet não podem sair livre de sanções, mas muitas delas saem, trazendo, além dos prejuízos patrimoniais, problemas psicológicos, depressão, baixa estima, síndrome do pânico, ansiedade e em alguns casos a vítima fica tão encurralada que tira a própria vida. O que precisamos compreender é que as ações que são tomadas virtualmente trazem consequências reais e estas muitas vezes atingem negativamente uma pessoa ou uma coletividade e precisa ser sanada.

As ferramentas utilizadas atualmente na internet como as redes sociais a exemplo do Instagram, *Whatsapp*, *Facebook*, *Twitter*, *TikTok*, são plataformas privadas que seguem políticas de uso independentes. As três primeiras citadas formam um conjunto de redes vinculadas a uma grande empresa controladora denominada Meta anteriormente chamada de *Facebook*. Todas possuem algoritmos que varrem a rede social em busca de palavras, imagens, áudios, vídeos que sejam de caráter discriminatório, vexatório, de ódio ou de qualquer outra forma de uso que possa atingir algum bem jurídico. Porém muitas vezes essas ferramentas não são suficientes para barrar crimes digitais fazendo com que o usuário lesado entre em contato com as redes sociais para que atitudes sejam tomadas e as mensagens, fotos ou outro tipo de mídia seja excluído e assim sanado o problema.

Porém, mesmo com as ações tomadas pelas empresas a vítima se sentir desemparada deverá procurar outros meios legais para assegurar seus direitos. Como os crimes cometidos em meio digital mais comuns são os crimes contra a honra, vale lembrar que esses tipos penais são de ação penal privada, ou seja, de iniciativa da vítima e o meio legal de procurar o jus puniendi do Estado é através de um requerimento na polícia civil ou diretamente na justiça através de uma queixa-crime.

> Essa forma de ação penal é de iniciativa do ofendido ou, quando este for menor ou incapaz, de seu representante legal. O direito de punir continua sendo estatal, mas a iniciativa da ação penal é transferida para o ofendido ou seu representante legal, uma vez que os delitos dessa natureza atingem a intimidade da vítima que pode preferir não levar a questão a juízo. (GONÇALVES, 2016, P. 146)

O requerimento nada mais é do que levar ao conhecimento da autoridade policial, fato pelo ofendido considerado criminoso. Este requerimento poderá ser realizado pelo próprio ofendido sem a obrigatoriedade de um advogado, mas nada obsta que um procurador seja constituído pelo ofendido para proceder o requerimento. O inquérito policial só poderá ser instaurado pela autoridade policial se existir requerimento feito por quem tem a titularidade da ação. Como se trata de crime de ação privada, o titular da ação é o ofendido, ou seu representante legal ou em caso de morte o cônjuge, ascendente descendente ou irmão.

“Art. 5º, §5º, CPP - Nos crimes de ação privada, a autoridade policial somente poderá proceder a inquérito a requerimento de quem tenha qualidade para intentá-la.” (PLANALTO)

Caso o ofendido resolva levar o caso diretamente para a justiça sem passar pela autoridade policial deverá fazê-la por meio de uma Queixa-Crime.

A Queixa-Crime é o nome da peça processual que dá início a ação privada e é sempre endereçada ao juízo competente. Após reunir todos os meios de prova que mostrem que alguém cometeu algum crime contra o ofendido, este terá o prazo de 6 meses contados da data que o crime foi descoberto para apresentar queixa-crime. Esta peça processual exige a presença de advogado com procuração com poderes especiais.

Se porventura o crime cometido por meio digital for de ação penal pública, o titular passa a ser o Ministério Público.

Ao se deparar com um crime digital, e se possível for, a primeira medida a ser tomada é a reunião de provas deste crime, reunir testemunhas, se o crime foi cometido em um site anotar seu endereço eletrônico. Atualmente um recurso muito útil em dispositivos computacionais e o *chamado print screen* que consiste em salvar uma imagem da tela do dispositivo em sua memória. Em grosso modo é tirar uma foto da tela do dispositivo e este recurso é essencial para que a vítima possa reunir provas do delito realizando prints de sites, conversas em redes sociais e fotos que ajudem na elucidação dos fatos. Deste modo, mesmo que o infrator apague seus atos, a vítima já terá copias em seu poder.

Com todos esses dados em mãos, o próximo passo é se deslocar até uma delegacia de polícia para realizar o requerimento ou ao juízo competente para apresentar queixa-crime. Porém por se tratar de crimes de ação pública privada e que na maioria das vezes ferem a honra, a dignidade e mancham o nome do ofendido perante uma sociedade, a vítima prefere não intentar contra o agressor temendo que os fatos ocorridos tomem proporções maiores do que já tenham tomado fazendo com que os problemas que fora sofridos com os atos aumente e traga mais transtornos, com isso ela se recusa em realizar requerimento ou queixa-crime e o agressor sai ileso do fato.

2.4 Lei 12.737/12 (lei dos crimes cibernéticos)

Carolina Dieckmann, atriz conceituada no âmbito nacional com diversas participações importantes em novelas, filmes e peças de teatro, em maio de 2012, teve seu computador invadido e fotos íntimas da atriz foram compartilhadas na internet. De início a atriz suspeitou que funcionários de uma empresa de assistência técnica tivessem copiado os arquivos e posteriormente divulgados quando ela deixou o aparelho na empresa para manutenção. Posteriormente fora comprovado que o delito teria sido cometido por invasores do estado de Minas Gerais e São Paulo, que enviaram um *SPAM* para o *email* da atriz que ao ser executado por ela, deu acesso para a entrada dos criminosos a seu dispositivo.

Anteriormente a este episódio, tramitava no Congresso Nacional o projeto de lei nº 2.793/11 que era uma alternativa para produzir legislação específica para crimes digitais. Este PL estabelecia menos tipos penais e deixava de lado questões polêmicas como a pornografia infantil dentre outros delitos.

Após o fato ocorrido com a atriz Carlina Dieckmann, a repercussão que esse fato trouxe para a sociedade, levando em conta a fama por trás da pessoa lesada e toda a importância que uma legislação específica poderia trazer para a sociedade o PL nº 2.793/11 começou a desbancar nas casas legislativas e transformou-se na Lei 12.737/12 que foi apelidada de Lei Carolina Dieckmann.

A principal atualização do Código Penal trazida pela 12.737/12 é percebida no Art. 154-A do CP que tipifica a invasão de dispositivo informático.

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (PLANALTO)

Analisando o amplo Art. 154-A podemos verificar que além do caput seus parágrafos abraçam diversos delitos relacionados a violações digitais. Apesar de apontar algumas falhas, a nova lei foi bem aceita pela classe doutrinária especializada pois trouxe consigo uma visão técnico-jurídica para vários tipos penais para que estes se enquadrem nos delitos praticados com novas tecnologias e que anteriormente são existiam forçando o julgador em alguns casos usar analogia *in malan partem*.

> "A cópia indevida de dados ou informações no Brasil era conduta sem tipo associado. Muitos promotores, em tais casos, ofereciam denúncias em face do crime de furto, previsto no art. 155 do Código Penal (subtrair, para si ou para outrem, coisa alheia móvel). Na doutrina, muitos asseveravam ser impossível a aplicação do tipo, considerando que a coisa “dados” não saía da esfera de disponibilidade da vítima, mas tão somente era “copiada”. Um “ctrl+c” não poderia ser considerado furto. Estes ajustes na legislação criminal são supridos com a Lei n. 12.737/2012, pelo art. 154-A do Código Penal" (JESUS, 2016, p.158)

A objetividade jurídica do delito tipificado no 154-A é a proteção da liberdade individual, do direito à intimidade e a segurança da informação protegendo os dados e informações pessoais.

> "Tutela-se a liberdade individual de manter íntegros os dados dispostos em preceito informático, bem como ilesos os próprios dispositivos em si, protegidos por mecanismo de segurança (a lei não esclarece o nível ou o tipo de segurança), de acessos não autorizados, expressa ou tacitamente, com a finalidade de:
>
> a) obter dados (objeto da alteração);
>
> b) alterar dados;
>
> c) destruir dados;

> d) instalar vulnerabilidade para obter vantagem ilícita." (JESUS, 2016, p.164)

A lei condiciona o delito a proteção do dispositivo de segurança contudo há uma divergência doutrinária em relação ao que pode ser considerado eficiente segurança do mecanismo. Para estes juristas, um aparelho celular de uma certa marca que tem como trava de segurança padrão a sequência 0000 para todos os aparelhos fabricados e que por descuido o usuário não altera este código e este dispositivo venha a ser violado não poderia se enquadrar no tipo penal em questão pois a ineficiência da senha é equivalente a uma ausência de proteção, e a ausência de proteção torna o fato atípico. Por outro lado, existe a corrente doutrinária que defende que o simples fato de possuir um mecanismo voltado para a segurança do dispositivo já é suficiente, pouco importando sua eficácia.

A lei 12.737/12 ainda trouxe outras atualizações para o código penal trazendo-o para mais próximo dos novos dispositivos de comunicação como vamos observar nos artigos 266 e 298 do CP.

Há época da criação da 12.737, os sistemas computacionais já estavam bem consolidados como ferramentas de comunicação, uma eficiente alternativa aos meios de comunicação tradicionais, porém não tinha a mesma proteção na legislação como tinha os serviços telefônicos por exemplo.

Foi a partir da inserção do parágrafo primeiro ao Art. 266 do Código Penal que sua proteção se materializou.

> Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
>
> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
>
> Pena - detenção, de um a três anos, e multa.
>
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (Incluído pela Lei nº 12.737, de 2012)

Outro ponto relevante que a lei 12.737/12 trouxe para o ordenamento jurídico foi a atualização do tipo penal referente à falsificação de documento particular

incluindo um parágrafo único ao Art. 298, com o objetivo de proteger documentos particulares em forma de cartões pessoais de crédito e de débito.

> **Falsificação de documento particular (**Redação dada pela Lei nº 12.737, de 2012) Vigência
>
> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
>
> Pena - reclusão, de um a cinco anos, e multa.
>
> **Falsificação de cartão (**Incluído pela Lei nº 12.737, de 2012) Vigência
>
> Parágrafo único. Para fins do disposto no **caput**, equipara-se a documento particular o cartão de crédito ou débito.

Nota-se que a atualização do Art. 298 foi um tanto quanto discreta, simples ao ponto de mencionar apenas cartões de crédito e débito e deixando de fora outros tipos de documentos particulares físicos e digitais como o *Token*, Certificado Digital, Cartões Virtuais dente outros.

> Para a caracterização do crime faz-se indispensável o exame de corpo de delito, sendo também imprescindível a apresentação do documento falsificado. A questão torna-se complexa quando a falsidade for informática, onde o plástico (cartão de crédito ou débito) permanece na posse da vítima, mas o atacante obteve acesso aos códigos e à numeração dos mesmos, fazendo-se passar pela vítima em sites e realizando compras em seu nome. (JESUS, 2016, p.233)

A cada dia que passa o documento físico está ficando mais precário, hoje temos cartões de crédito, débito, carteira nacional de habilitação, CPF, assinaturas, documentos de veículos todos em formato digital e isso passa a ser mais um desafio para o ordenamento jurídico enfrentar.

É sabido que o direito evolui ao passo que a sociedade evoluir, porém a velocidade em que a tecnologia da informação evolui é muito rápida e nota-se que de alguma forma o direito não consegue acompanhá-la em tudo deixando lacunas na legislação.

2.5 Lei 12.965/14 (marco civil da internet)

A lei nº 12.965/14, aprovada na Câmara dos Deputados em 25 de março de 2014 e no Senado Federal em 23 de abril de 2014, foi regulamentada com a intenção de resguardar princípios em ambiente virtual já assegurados no ambiente real bem como estabelecer o papel da União, Estados, Distrito Federal e Municípios nestas regulamentações.

Um detalhe que chama a atenção nesta lei é que o conteúdo nela expresso foram elaborados com a participação popular por meio de debates e audiências públicas pelo país.

Apelidada de Marco Civil da Internet, a lei 12.965/14 surgiu para suprir a necessidade do ordenamento jurídico em acompanhar a evolução tecnológica e da sociedade da informação e com isso diminuir cada vez mais o aspecto de terra sem lei que paira sobre a internet. Esta atitude se deu no momento em que percebeu-se que as ações da sociedade em meio digital trazia consequências ao mundo real e estas ações precisavam ser abraçadas pela legislação.

> "O Marco Civil da Internet é considerado a “Constituição da Internet”, garantindo direitos e deveres a todos os atores da Internet brasileira (usuários, provedores de conexão e de serviços em geral). Fruto de um projeto nascido em 29 de outubro de 2009, da Secretaria de Assuntos Legislativos do Ministério da Justiça, em parceria com a Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, o Marco Civil foi uma construção colaborativa, disponível para consulta pública entre novembro de 2009 e junho de 2010, tendo recebido mais de duas mil contribuições" (JESUS, 2016, p.354)

A lei em questão possui 32 artigos divididos em 5 capítulos que trazem consigo as garantias referentes a privacidade, neutralidade e do armazenamento de registros de acesso. A lei ainda trata do armazenamento de informações pessoais dos usuários pelos sites devendo estes respeitar as garantias para este tipo de atitude.

Partindo do princípio da legalidade que diz que ninguém é obrigado a fazer ou deixar de fazer algo senão em virtude de lei, até a chegada do Marco Civil da Internet, não existia lei nacional que obrigasse provedores de internet ou de serviços a registrarem os dados das atividades dos usuários em suas plataformas, com isso muitos delitos passavam impunes pois sem registros de atividades e levando em consideração que quem acessa um site ou qualquer outro ambiente virtual para cometer crimes, entra de forma anônima (não utiliza seus dados pessoais verdadeiros) fica praticamente impossível chegar até o infrator.

Em seu Art. 11º a lei 12.965/14 traz consigo a garantia da inviolabilidade, da confidencialidade e do sigilo das relações virtuais dos usuários, porém também traz a exceção para quebra do sigilo por ordem judicial, com isso, se em algum delito, for

relevante para a investigação a coleta dos registros de acesso e dados pessoais do infrator este artigo garante a quebra.

> Art.11º. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em 31 território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

O Marco Civil da internet trouxe consigo a regulamentação da proteção contra a violação de informações pessoais para que terceiros não utilizem esses dados para fins diversos.

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I – Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei.”
> [...] VIII- Informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.

Do mesmo modo da Lei Carolina Dieckmann, o Marco Civil da Internet trouxe contribuições importantes e benéficas atualizações para o ordenamento jurídico nacional, deixando-o cada vez mais próximo do ambiente virtual e da era digital em que vivemos, contudo, ainda não é o suficiente para resguardar completamente os dados pessoais dos usuários devido a lacunas em suas normas.

2.6 Lei 13.709/18 (lei geral de proteção de dados)

A lei 13.709/18 denominada Lei Geral de Proteção de Dados tem como objetivo a proteção de direitos fundamentais de liberdade e de privacidade. Foca também na padronização da regulamentação e no aspecto prático trazendo com isso mais proteção aos dados pessoas dos residentes no Brasil seja ele brasileiro ou estrangeiro proporcionando um cenário de segurança jurídica.

A lei visa regular a proteção dos dados pessoais, seja ela pessoa física ou pessoa jurídica garantindo direitos aos cidadãos e impondo regras sobre as operações que tratam de dados pessoais realizadas por entidades públicas ou privadas podendo a vítima em caso de danos sofridos em decorrência de vazamento de dados, ser indenizada.

A criação da lei se deu devido às suspeitas de que os dados dos usuários da rede estivessem sendo utilizados de maneira indevida necessitando de um dispositivo a fim de evitar abusos em relação a intimidade das pessoas.

Ao se criar uma cota no *Google* para ter acesso às ferramentas da empresa, o usuário informa alguns dados que aparentemente não compromete sua intimidade, os mais comuns são: nome completo, data de nascimento e gênero. Após confirmado os dados o usuário passa a ter acesso às ferramentas da empresa utilizada aqui como exemplo. Este usuário poderá usar esta conta do *Google* para ingressar em uma rede social com o Instagram por exemplo. A partir do momento que a conta do *Google* é usada para criar o perfil do *Instagram* há uma troca de informações entre as empresas, estas informações são armazenadas em um banco de dados e o usuário não tem ideia de como esses dados serão utilizados. Se pararmos para refletir com apenas o nome completo, data de nascimento e gênero uma rede social saberá que o usuário é sul-americano, europeu, asiático, se é um adolescente, adulto ou idoso, se é homem mulher. Esses dados são de grande valia para a rede social porque através deles é que virão os anúncios de empresas ao perfil do usuário e com as informações passadas se diminui a chance de mostrar um produto ou um serviço ao usuário que não seja do seu interesse.

Nos últimos tempos vimos casos de vazamento dessas informações pessoais de milhares de usuários de redes sociais e isso é extremamente preocupante pois em alguns casos os usuários informam CPF, endereço e diversos outros dados pessoais e esses vazamentos podem levar esses dados para locais não sabidos e utilizados para fins ilícitos.

Um caso de grande repercussão mundial aconteceu nos Estados Unidos onde dados sigilosos de 50 milhões de usuários norte-americanos do *Facebook* foram vazados para uma empresa de *marketing* que ajudou a eleger Donald Trump, presidente do país em 2016.

> A empresa em questão, Cambridge Analytica, praticou o roubo dos dados através do aplicativo This is your digital life, criado por um desenvolvedor de aplicativos chamado GSR. O programa disponibilizava aos usuários uma série de perguntas e em troca eles deveriam consentir o acesso às suas informações como localização e curtidas. Cerca de 270 mil pessoas disponibilizaram seus dados dessa forma, porém, além dos dados desses usuários, o aplicativo captava as informações de todos os seus amigos, totalizando cerca de 50 milhões de pessoas. A rede social em questão, após o acontecido, retirou o aplicativo do ar e solicitou a eliminação dos dados obtidos (TAVARES, 2018).

No Brasil ocorreu um vazamento de dados pessoais dos usuários do *Facebook* através da mesma empresa do vazamento norte americano, a *Cambridge Analytica* conseguiu acesso aos dados privados de pelo menos 443 mil brasileiros do *Facebook,* mas ao contrário do que ocorrera nos Estados Unidos, os dados dos brasileiros não foram utilizados por práticas abusivas, mas apenas ficaram disponíveis indevidamente no banco de dados dos desenvolvedores do aplicativo *thisisyourdigitallife*.

> O Brasil decidiu multar o Facebook em 6,6 milhões de reais pelo vazamento de dados de ao menos 443.000 usuários brasileiros. A decisão foi do Ministério da Justiça e Segurança Pública, que, por meio do Departamento de Proteção e Defesa do Consumidor, aplicou a multa em razão do compartilhamento indevido de dados de usuários brasileiros no caso Cambridge Analytica. (ROSSI, 2018)

Este episódio do vazamento de dados dos brasileiros foi o estopim para a movimentação para a criação de uma lei que evitasse abusos que causassem aos direitos de privacidade e de intimidade dos usuários.

3 DIFICULDADE NA APLICAÇÃO DE SANÇÕES AOS INFRATORES

Como a tecnologia da informação está em constante evolução, é de se compreender as dificuldades que o processo investigatório e o processo judicial sofrem para solucionar delitos ocorridos digitalmente. Porém o Estado não pode ficar inerte sem buscar melhorias que possam amenizar a distância tecnológica entre o poder investigatório e o fato criminoso cometido digitalmente. Como já podemos perceber no capítulo anterior, novas legislações vêm sendo criadas com a intenção de afunilar cada vez mais as lacunas legais que existem tornando mais efetiva a solução dos crimes digitais mais ainda tem um longo caminho a ser percorrido.

Muitos dos crimes digitais são praticados por pessoa com conhecimento técnico na área, montando verdadeiras estratégias e seu planejamento pode se arrastar por dias. Uma característica interessante dos crimes digitais próprios que envolve fraude computacional ou furto de dados é que estes são praticados na mesma velocidade do processamento de dados, ou seja, em poucos milissegundos, passando despercebido pela vítima que só virá perceber o delito após detectar prejuízos futuros. Estes crimes são praticados por delinquentes de característica inteligente, gentil e educada com bagagem técnica na tecnologia da informação.

Quando passamos a falar dos crimes digitais impróprios, aqueles que usam a tecnologia apenas como meio para se atingir um bem jurídico, consideramos que o

infrator pode ser qualquer pessoa com conhecimento básico na operação de um dispositivo. Com isso o leque de suspeitos se torna imenso pois ao contrário dos crimes próprios que o investigador pode delimitar as pessoas investigadas pela capacidade técnica em informática, nos crimes impróprios o leque se torna praticamente toda a sociedade. Pontos que dificultam o processo investigatório de crimes digitais são a ausência física do agente, como o crime é praticado com o uso de um sistema computacional, dificilmente será visto um agente físico perpetrando o delito, a dificuldade para delimitar a extensão do crime, a falta de colaboração das vítimas com as autoridades investigativas, a ausência de denúncias e o pouco aparato técnico especializado disponíveis às autoridades.

> Um procedimento muito importante realizado por equipes de investigação é a chamada “busca sistemática”. Esse modelo de investigação de crime na internet é uma forma de investigação preventiva, dependendo apenas da iniciativa da autoridade responsável pela condução do procedimento, no qual são identificados responsáveis por diversos tipos de crimes. A falsa sensação de anonimato provocada pela internet, facilita esse meio de investigação. Contudo, os investigadores têm que definir parâmetros e impor limites a essa metodologia, já que o grande volume de informação pode gerar lentidão ao processo e tomar muito tempo (BRASIL, 2016).

Compreendemos a situação benéfica que a evolução da internet trouxe para a sociedade, porém com os benefícios vieram novos delitos, condutas que ferem princípios morais e novas formas de praticar crimes já conhecidos e tipificados em nosso ordenamento jurídico.

Essas modalidades de crimes não param de crescer no Brasil, sempre evoluindo e dificultando a aplicação de sanções aos infratores, facilitada pelo anonimato da rede mundial de computadores, falta de aparato especializado para o combate além de análises técnicas na tipificação dos delitos. Isso torna essencial a busca da população e dos legisladores por mecanismos de prevenção de crimes e a sanção para os criminosos.

> A internet facilita a impunidade, uma vez que a investigação é mais complicada e, muitas vezes, quando é identificado o autor, já ocorreu a prescrição. Isso sem contar na questão da fronteira: o crime pode ser cometido por alguém que está em outro país, com leis completamente diferentes. A fronteira acaba motivando também, de certa forma, a impunidade. E aqui, infelizmente, não tem muito o que

> fazer. Porque não tem como criar uma lei obrigando o cidadão da Estônia a vir para o Brasil no prazo. (BURG, 2017)

Na visão de BURG, a internet e sua magnitude facilita a impunidade por ser mais fácil para o criminoso se esconder e se deslocar dentro dela do que no mundo real por exemplo. Isso dificulta a investigação pois os agentes responsáveis por investigar muitas vezes quando se atentam aos fatos o crime já tem entrado em prescrição. A questão da territorialidade atrapalha também haja vista a facilidade que o infrator tem de se comunicar com qualquer parte do mundo através da internet, podendo ele estando no Japão, acessar remotamente um dispositivo na Colômbia e deste dispositivo cometer um crime na Rússia por exemplo, tornando dificultoso a busca real do infrator.

> A legislação brasileira não está adequada e, muitas vezes, o crime prescreve sem que haja um avanço significativo nas investigações. Nos crimes contra a honra, por exemplo, há uma enorme dificuldade para se identificar o autor de ofensas realizadas na internet, e sem a identificação sequer é possível oferecer queixa-crime. (BURG, 2017)

Existe uma dificuldade considerável no que tange a punição dos agentes que cometem crimes contra a honra nas redes sociais por exemplo. Mutas pessoas criam perfis falsos com o dolo de atacar a honra alheia nas redes sociais e mesmo estando a ofensa ali publicada, materializando o crime, as lacunas nas nossas leis específicas deixam a punição em aberto como também a não identificação do agente faz com que a queixa-crime, peça de entrada para ações penais privadas, fique impossibilitada de ser oferecida.

3.1 Perfil e identificação dos criminosos

Não há consenso quando se fala em traçar um perfil de um criminoso digital, o que sabemos é que no Brasil a cada dia que passa o crime digital se torna mais criativo e menos técnico. Isso implica dizer que pessoas sem grau elevado de conhecimento em informática vem cometendo tais delitos.

Tempos atrás, um criminoso digital era visto como um gênio da computação que utilizava suas habilidades técnicas para invadir e fraudar sistemas computacionais. Este cenário vem se modificando e atualmente grande parte dos delitos cometidos na internet se deve ao pouco conhecimento de quem usa as ferramentas, despreparo técnico dos agentes de investigação e a facilidade de

acesso às técnicas e ferramentas para a prática destes delitos. O que se percebe é que os criminosos digitais não são pessoas que cometem crimes no mundo real, eles se aproveitam da falsa sensação de anonimato, do desconhecimento dos usuários e da imperícia dos investigadores para atuar neste ambiente. Não é à toa que há uma crescente na quantidade de jovens de classe média e alta envolvidos em crimes digitais.

> Logo, muito se fala em “crimes de alta tecnologia” quando, na verdade, a tecnologia utilizada na maior parte dos casos é trivial, corriqueira, de fácil curva de aprendizagem, e com ferramentas disponíveis para venda e troca em redes IRC (Internet Relay Chat) e demais cantos da Internet. Horas de vídeos disponíveis na Internet podem conduzir pessoas a praticarem invasões com relativa facilidade. As vítimas comumente contribuem e cooperam ativamente para se tornarem vítimas, facilitando o trabalho do cibercrime. (JESUS, 2016, p.96)

Como visto, não temos uma padronização no perfil do criminoso digital e é consideravelmente compreensível haja vista a quantidade de crimes que de alguma forma possam vir a ser cometidos digitalmente, no ambiente real o perfil de um estuprador nada se compara ao perfil de um estelionatário e como já vimos, esses dois delitos também podem ser cometidos em meio virtual e não seria lógico traçar um perfil igual para esses dois infratores.

Quando se trata de crimes digitais próprios fica mais fácil traçar um perfil empírico dos criminosos pois estes crimes exigem mesmo que mínimo, um pouco mais de conhecimento técnico do que os crimes digitais impróprios.

> O perfil do criminoso, baseado em pesquisa empírica, indica jovens, inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, ‘uma brincadeira’. Mais: preferem ficção científica, música, xadrez, jogos de guerra e não gostam de esportes, sendo que suas condutas geralmente passam por três estágios: o desafio, o dinheiro extra e, por fim, os altos gastos e o comércio ilegal. (JESUS, 2016, p.97)

Os jovens têm por natureza a aventura e a liberdade inconsequente no sangue, e isso é um belo combustível para que alguns se envolvam no mundo do crie sem pensar nas consequências. É sabido que jovens pobres e com poucas

oportunidades sociais têm uma probabilidade imensa de entrar na criminalidade por não ter nada a perder e querer algo na vida mesmo que seja por vias ilícitas. Mas o que ocorre nos crimes digitais é o alto número de jovens de classe média alta envolvidos no crime munidos pela aventura e pelo desafio de invadir sistemas e cometer fraudes digitais encobertos pela falsa cortina do anonimato e da impunidade.

CONSIDERAÇÕES FINAIS

A evolução da tecnologia, em especial as que trouxeram inovação para a comunicação e para o processo de dados informáticos entraram rapidamente no cotidiano da sociedade, com isso vieram fatos até antes desconhecidos que de alguma forma prejudicava um indivíduo ou uma coletividade, podemos dizer que os crimes digitais se enquadram nesses fatos.

Diante da elaboração deste texto, foi levantada a questão da definição de crimes digitais, mostrando de forma coesa a que se referem enfatizando o assunto procurando mostrar as condutas tidas como criminosas como mostrando os delitos mais comuns neste ambiente.

Com relação a classificação dos crimes digitais observou-se uma divergência doutrinária a respeito do tema, mas analisando a corrente majoritária chegamos a uma definição desta classificação. Observou-se que no Brasil o crime digital mais comum atualmente são os crimes impróprios que ferem a honra do ofendido. Fora apontados os crimes de calúnia, difamação e injúria como os mais comuns entre os delitos digitais mais praticados claro, sem deixar de mencionar outros tipos penais.

Observou-se também a dificuldade de investigação destes crimes e a deficiência na colheita de indícios de autoria.

Constatamos que mesmo com a evolução da legislação que vem ganhando leis importantes principalmente a partir de 2012 que amparam os crimes digitais, nota-se também uma fragilidade nestes códigos, lacunas nas leis e em alguns casos textos abstratos e pouco efetivo que prejudicam o processo investigatório e a efetiva punição dos criminosos. Estas falhas não podem se manter perante a constante evolução tecnológica pois a cada dia aumenta as demandas de processos que clamam por soluções e de pessoas que são vítimas de delitos digitais e ficam sem solução para os crimes que foram praticados contra elas.

Se faz necessário a criação de lei específica atuando de forma geral, baseada nos crimes denunciados que não apresenta soluções concretas por falta de legislação. Por outro lado, pouco se resolve com a produção legal se em conjunto não for aprimorado os meios de investigação, seus equipamentos e a capacitação técnica dos envolvidos.

Por fim considera-se que o presente trabalho conquistou o objetivo proposto ao tempo que mostrou a caminhada digital na sociedade, respondendo os questionamentos levantados. Tornando a leitura recomendada para estudantes do curso de Direito, Ciências da Computação ou para estudantes de outras áreas acadêmicas que tenham interesse nos conhecimentos aqui transmitidos.

REFERÊNCIAS

BRASIL. **Curso Crimes Cibernéticos: procedimentos básicos**. SENASP/MJ, 2016. Disponível em: http://portal.ead.senasp.gov.br/academico/copy_of_editoria-a/crimes-ciberneticos-nocoes-basicas. Acesso em 23 de novembro de 2021.

Brasil é o 5ª maior alvo de crimes digitais no mundo em 2021. Canal Tech, 2021. Disponível em:https://canaltech.com.br/seguranca/brasil-e-o-5o-maior-alvo-de-crimes-digitais-no-mundo-em-2021-195628/. Acesso em: 15 de outubro de 2021.

BRUG, Daniel Allan. **Internet facilita crimes e dificulta investigação, estimulando a impunidade**. Conjur, 2017. Disponível em:https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais. Acesso em: 26 de novembro de 2021.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2017.

JESUS, D. D. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016. *E-book*.

Direito digital: tudo o que os advogados precisam saber. SajAdv, 2020. Disponível em:https://blog.sajadv.com.br/tudo-sobre-direito-digital/. Acesso em 19 de outubro de 2021.

Golpe do falso intermediário é um dos mais usados no mercado de compra e venda de carros usados. Fantástico, 2021. Disponível em: https://g1.globo.com/fantastico/noticia/2021/10/24/golpe-do-falso-intermediario-e-um-dos-mais-usados-no-mercado-de-compra-e-venda-de-carros-usados.ghtml. Acesso em: 26 de novembro de 2021.

PACI, Maria Fernanda. Considerações gerais dobre o direito eletrônico. **Âmbito Jurídico**, 2017. Disponível em:https://ambitojuridico.com.br/edicoes/revista-162/consideracoes-gerais-sobre-direito-eletronico/. Acesso em: 24 de outubro de 2021.

PECK, Patrícia. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2015. E-book.