CRIMES VIRTUAIS: uma abordagem de práticascriminosas na *internet* à luz da lei 12.737/2012

NYCOLAS GAVA BAESSO TREUHERZ[1]
KAULLY FURIAMA SANTOS[2]

RESUMO: Os crimes virtuais, estão aumentando cada vez mais, seja as entidades públicas ou privadas e principalmente na *deep web*. Esses criminosos ficam protegidospela possibilidade de anonimato e imensidão da internet, tornando difícil a aplicação e adefinição das leis que possam punir tais criminosos, protegendo assim a sociedade. Coma evolução da *internet*, a sociedade tornou-se dependente dessa tecnologia, pois ela nospropicia diversas facilidades, no entanto, é onde os criminosos se aproveitam dessa tecnologia para praticar os crimes, que afetam não apenas um indivíduo, mas, toda a população. O objetivo geral deste trabalho foi demonstrar a necessidade de uma legislaçãoespecífica para fiscalizar e coibir com abrangência e eficácia os crimes que se utilizamdos meios virtuais de atuação. A metodologia utilizada neste trabalho foi a bibliográfica.Com tudo, o avanço no uso da informática e da internet para os mais diversos fins é constatado que, juntamente com as facilidades e os benefícios, as ações criminosas quefazem uso das mesmas tecnologias crescem em igual proporção. Este cenário faz premente a evolução da legislação no sentido de abordar as características destes crimesque passam a acontecer pelo meio virtual, utilizados como instrumentos de ação o computador em si, contas de *e-mail*, ambientes de transação, compra e venda pela *internet*, além de ferramentas elaboradas no intuito exclusivo de burlar a segurança digital das redes de computador
PALAVRAS-CHAVE: Crime virtual. Legislação. Internet.

VIRTUAL CRIMES: an approach to criminal practices on the internet in the light of law 12.737/2012

ABSTRACT: Virtual crimes are increasing more and more, whether public or private entities and mainly on the deep web. These criminals are protected by the possibility of anonymity and the immensity of the internet, making it difficult to apply and define laws that can punish such criminals, thus protecting society. With the evolution of the internet, society has become dependent on this technology, as it provides us with several facilities, however, it is where criminals take advantage of this technology to commit crimes, which affect not only an individual, but the entire population. . The general objective of this work was to demonstrate the need for specific legislation to comprehensively and effectively monitor and curb crimes that use virtual means of action. The methodology used in this work was the bibliographical one. With everything, the advancement in the use of information technology and the internet for the most diverse purposes it is verified that, together with the facilities and benefits, the criminal actions that make use of the same technologies grow in equal proportion. This scenario urges the evolution of legislation in order to address the characteristics of these crimes that happen in the virtual environment, using the computer itself, e-mail accounts, transaction environments, buying and selling over the internet, as instruments of action. in addition to tools designed exclusively to circumvent the digital security of computer networks
KEYWORDS: Cybercrime. Legislation. Internet.

[1] Acadêmico de Graduação, Curso de Direito, Faculdade de Sinop-FASIP, Endereço eletrônico:nycolasgava@outlook.com;
[2] Professor Mestre em Direito, Curso de Direito, Faculdade de Sinop-FASIP, Endereço eletrônico:kfuriama@gmail.com;

INTRODUÇÃO

A realização da presente pesquisa busca mostrar conceitos sobre crimes virtuais. Que ocorrem desde o ano 1970. Com o avanço e acessibilidade da internet houve o aumento dos delitos, evidenciando a fragilidade da aplicação do Código Penal [1](1940) eCódigo Civil (2002) para as ocorrências. Com avanço da tecnologia o sistema de *internet* se tornou um bem social capaz e eficaz com facilidade em vários ramos da sociedade.

Como se tornou de fácil utilização e acesso, a insegurança e os transtornos causados utilizando a internet só aumentam a cada ano. Se faz necessário a criação de uma legislação específica, coercitiva abrangente onde o legislador possa criar a partir dos casos existentes e previsíveis uma lei eficaz nas mais diversas possibilidades. As falhasna regulamentação existente são falhas por falta de especificidade e por não alcançar olado obscuro onde os criminosos atuam, como é o caso da navegação na *deep web (undernet)* (VIEIRA, 2018, n.p.).

É necessária uma legislação com especificações no ambiente virtual, com punições proporcionais. A Lei 12.737/2012, também conhecida como Lei Carolina Dieckmann modificou o Código Penal, juntamente com o marco civil, Lei 12.965/2014 ea LGPD Lei n° 13.709/2018, entretanto, as interpretações são dúbias e brandas. O uso incontrolado da *undernet (deep web)* acaba dificultando o rastreio dos criminosos e o aumento da impunidade. Sendo, necessária uma fiscalização de efetividade e controle sobre esses acessos, se fazendo necessária regulamentações mais severas (PINHEIRO,2017, n.p).

Com o avanço do mundo globalizado onde a informação está cada vez maior, omundo virtual está sofrendo alterações e regulamentação. Contudo, para muitos ainda éconhecida como "terra sem lei". O estudo tem por objetivo responder a seguinte pergunta: O Código Penal brasileiro (1940) é capaz de conter o crescente número de impunidadesque os usuários da internet vêm sofrendo, ao longo dos anos?

O objetivo geral deste trabalho foi demonstrar a necessidade de uma legislaçãoespecífica para fiscalizar e coibir com abrangência e eficácia os crimes que se utilizamdos meios virtuais de atuação e os objetivos específicos foram apresentar a evolução histórica dos avanços e ampliação dos meios de comunicação com a implantação da internet, demonstrar de forma clara as lacunas nas legislações existentes e explicar de forma objetiva a necessidade da regulamentação sobre *undernet*.

As pesquisas foram feitas em livros da doutrina, leis, artigos, trabalhos científicos e jurisprudência dos principais tribunais do país. O método inicial foi o levantamento dos trabalhos acerca do tema, para que fosse realizada a revisão bibliográfica. O método utilizado foi o qualitativo e descritivo, abrangendo leis, trabalhos científicos, doutrinas e jurisprudências. Estes, por sua vez, foram consultados em livrosfísicos, sites especializados de direito e sites dos tribunais superiores. Logo, com base nos dados qualitativos a serem obtidos na revisão bibliográfica, analisar-se-á qual direito preponderar.

2. REVISÃO DE LITERATURA

2.1 A evolução histórica dos avanços e ampliação dos meios de comunicação com a implantação da *internet*

O computador tem o potencial para ser a ferramenta que vai impulsionar a inteligência humana num futuro próximo. É o que vem acontecendo. O caminho percorrido do desenvolvimento da sociedade com os avanços, agilidade e praticidade proporcionado pela tecnologia e suas constantes modificações e acessibilidade de informações em tempo real a nível mundial através da *internet* (WU, 2016, n.p.).

O caminho percorrido do desenvolvimento da sociedade com os avanços, agilidade e praticidade proporcionado pela tecnologia, com o surgimento da internet nãose havia registro sobre o tema "Crimes Virtuais". Conhecido como furto de dados, os crimes virtuais eram

enquadrados no delito furto do Código Penal (1940).

De modo que os crimes de extorsão, ameaça, furto, estelionato já haviam tutelano Código Penal (1940) a diferença está nos meios do cometimento da infração, podendo serem crimes virtuais próprios, o qual o agente do crime utiliza de computador para pratica-los.

Da mesma forma que a internet possibilita todo este conjunto de conteúdo e ferramentas que favorece a pesquisa, o desenvolvimento humano, o trabalho, o comércioe as relações em geral, a internet também ensejou a prática de condutas ilícita, e, nesteponto, cria-se um problema, já que, embora boa parte dos crimes cometidos virtualmentejá seja existente no mundo então denominado real, outra parte não se enquadraperfeitamente em nenhum deles, ou seja, é tido como desconhecido e, portanto, pode carecer do adequado amparo da lei (LÉVY, 2016).

A partir de então, a rede passou por diversos estágios de evolução, deixando deatender a fins somente militares e se popularizando, passando a ser utilizada com diversos propósitos e a vislumbrar usuários das mais diversas áreas. Atualmente, inúmeras definições e conceitos são encontrados acerca da internet em livros, trabalhos acadêmicose na própria rede.

2.1.1 Funcionamento da Internet

Como ora entendido, a *internet* é caracterizada por uma gigantesca rede de computadores e todo o equipamento e tecnologia agregados para que se dê seufuncionamento e utilização. No entanto, seria impossível manter uma rede de tamanha grandeza sem a existência de sistemas de organização estruturados (NOGUEIRA, 2018,n.p.).

Dois pontos específicos merecem desdobramento. No que o autor se refere a certas condições, pode-se entender que o acesso não é livre e desimpedido a qualquer computador interligado. Caso assim fosse, a segurança das informações de cada usuárioestaria seriamente comprometida. Existem protocolos e sistemas que gerenciam as permissões e direcionam os usuários aos endereços onde pode ingressar, dentro de rigorosos métodos de segurança e autenticação.

Assim esclarece Fraga, (2019), ao colocar que o computador, então conectado,passa a ser identificado por um endereço lógico que permita sua localização e certificação. Tal endereço, especificado por parâmetros próprios da informática, define tanto o computador que visita como o que é visitado. Trata-se de um endereço composto por números e denominado *Internet Protocol - IP*.

Porém, em contraponto, a utilização se dá por interfaces intuitivas e simples, ficando todo o aspecto técnico oculto por trás de layouts amigáveis e de bom entendimento. E, por fim, cabe ressaltar que apesar de todo o investimento que se faz em aspectos de segurança, a internet ainda é, assim como todos os lugares não virtuais, sujeitaa crimes das mais diversas naturezas.

2.1.2 A Importância da Internet na Atualidade

Com a crescente explosão de acesso de usuários na rede, maiores foram os casos de crimes cometidos neste ambiente virtual. Não se tratando apenas de um ambiente comum somente de pesquisas, mas também, de um local de possíveis negócios jurídicose, de relações de consumo, no chamado comércio eletrônico, com o oferecimento de serviços profissionais bem capacitados, possíveis de realizar transações de mercadorias e ainda negociações de títulos executivos na bolsa de valores, como a compra e venda deações, motivo pelo qual se deu extrema importância para sua utilização nos tempos atuais (FRAGA, 2019).

Saltando para outro ponto, a internet no ramo do trabalho, desenvolveu grandedestaque por gerar uma cadeia produtiva de serviços em casa, gerando assim, diversasformas de lucros por serviços online.

Aliado a todo esse processo, a evolução tecnológica desenvolvida através da internet, trouxe fundamental importância até para a Justiça, através de mudanças ocorridas com a transposição do processo impresso para o processo digital. Modificando assim, os atos processuais em suas petições, despachos, sentenças, etc., com um sistemaprocessual específico resguardado pela lei 11.4198 de 19 de dezembro de 2006, que dispõe sobre a informatização do processo

judicial (VIEIRA, 2018).

Apesar de todos esses avanços, paralelo a isto, tem-se aumentado um númeromaior de atividades criminosas. Visto isto é visível a importância desse sistema no mundo contemporâneo, pois seria impossível imaginar a vida sem todas as praticidades e confortos que a internet proporcionou.

2.2 O *Cibercrime*

Fraga (2019, n.p.) conceitua crime como uma conduta típica (a ação ou omissão praticada pelo sujeito deve ser tipificada, isto é, deve ser descrita em lei como delito) eantijurídica (conduta ilícita, contrária ao direito).

A Constituição da República Federativa do Brasil (1988), em seu artigo 5º, incisoXXXIX, determina: "Não há crime sem lei anterior que o defina, nem pena sem préviacominação legal". Diante disso, com o passar do tempo e o surgimento de novas tecnologias, também a legislação vem sendo atualizada para abranger novas condutas criminosas.

O exemplo mais recente é a Lei 12.737/2012 que criminaliza, dentre outras, aconduta de invadir e infectar computadores alheios com *malwares*, conduta esta que, embora nociva, até então não era considerada crime. Não foi encontrado um texto legalque defina delito informático, tendo sido trazidas definições dadas pelos autorespesquisados, entendendo-se como sinônimos: crimes de informática, *cibercrime*, crime cibernético, ou ainda, crime digital (CASELLI; WENDT, 2017).

Crime digital é a utilização de computadores para ajuda em atividades ilegais, subvertendo a segurança de sistemas, ou usando a internet ou redes bancárias de maneirailícita. Para o referido autor, a classificação mais objetiva é a que divide os delitos em próprios e impróprios.

Crimes digitais próprios, segundo Vieira (2018). São todas as condutas praticadas contra bens jurídicos informáticos, tais como sistemas e dados (os meios eletrônicos são o objeto protegido); crimes digitais impróprios são as condutas dirigidascontra bens jurídicos tradicionais, não relativos à tecnologia, porém, utilizando-se meiostecnológicos como instrumento.

Trata-se de uma conceituação abrangente, genérica, e que pode dar margem para especulações e tentativas de burla. É de se alertar sobre a falta de conhecimentos básicos acerca do assunto por parte do legislador, e ressalta sua observação lembrando que, atualmente, o Código Criminal não traz uma conceituação para crime, tendo esta ficadorelegada é possível apenas através de buscas de disposições espalhadas pelo próprio código.

Percebe-se que, para enquadrar um ato em uma das definições mencionadas, faz- se necessária sua interpretação, a fim de que se garanta a tipificação, ou seja, que realmente se encaixa no conceito de crime e deve ser punido. O problema é que tal interpretação abre margem para discussão, dado o caráter vago impróprio.

Porém, ainda assim impróprio, Fraga (2019) afirma a possibilidade de um fatoser típico, antijurídico, culpado e ameaçado com pena *in thesi*. Ou seja, ser criminoso, mas não acarretar a imposição da pena, como em casos de furto familiar, favorecimento pessoal e extintivas condicionais, em que existe crime, mas sem aplicação de pena.

Partindo do conceito analítico, seria correto afirmar que crime virtual é caracterizado por ação típica, antijurídica e culpável cometida contra ou através de meios informatizados, ou seja, que envolvam o processamento ou a transmissão de dados. A Organização das Nações Unidas (ONU) apresenta definição semelhante: qualquer conduta ilegal não ética ou não autorizada que envolva processamento automático de dados e/ou transmissão de dados (CASELLI; WENDT, 2017).

A partir deste simples exemplo e vislumbrando os tantos outros que semelhantemente poderiam ser elencados, percebe-se a complexidade quanto à tipificação, e esta, quando abordados fatos de elevada complexidade, podem conduzir adificuldades de julgamento e de enquadramento na lei.

2.3 Ciberespaço como Virtualização Realidade

A cidade é algo que a humanidade possui que se pode dizer como um local mais elevado como objetivo de moradia. A cidade é um local onde se vive em comunidade ocupado e compartilhado por pessoas, com o intuito de promover uma condição de vidaagradável. Com isso a cidade deverá promover algo que venha a satisfazer as necessidades humanas (CAPEZ, 2015, n.p.).

Na perspectiva do presente trabalho, pelo fato de o homem ser um animal sociale, portanto, busca incessantemente o envolvimento com grupos sociais, dos quais podevir a fazer parte, seja por escolha própria ou por determinação do meio em que vive. Aotornar-se parte de um agrupamento social é mister que o homem siga as regras estabelecidas com o fim de promover a ordem e a justiça no grupo em questão(BARRETO; BRASIL, 2016, n.p).

2.3.1 Virtualização do Espaço Comunitário

Dentre as diferentes maneiras de contato e comunicação social, as redes sociais*on-line* estão entre uma das formas mais utilizadas para as relações sociais. Contudo elaé apenas uma vertente do que se pode chamar de ciberespaço.

Conforme Mucheroni e Martinez (2013), o conhecimento de ciberespaço leva ànoção de cibercultura. Todo ser humano nasce e cresce se desenvolvendo ao meio de um contexto prenotado de relações interpessoais. Estes se englobam de forma inevitável, em composto de normas que pré-estabelecem o comportamento de quem ali faz parte.

Contudo o ciberespaço traz consigo um comportamento onde se altera tais comportamentos, neste espaço virtual as pessoas se relacionam de forma livre e sem regras ou ideais, com isso sabe-se que é inevitável uma criação de comportamentos.

Rede social é um local que consiste em uma relação de pessoas que estão ligadas por algum objetivo, seja ela política, comunitária, profissional, pessoal, lazer entre outros. As redes sociais sempre existiram até mesmo antes da internet, pois o ser humano é umser que tem por instinto próprio a necessidade de se relacionar, seja essa relação qual for.Cria-se ali uma lista de amigos, conhecidos e até mesmo desconhecidos que têm acessosa todas essas informações (Tomaél, Alcará e Di Chiara, 2014).

Uma das diversas características nas redes sociais são as de se identificar criando um perfil colocando ali informações pessoais, informações de preferências sejam elas preferencial de lazer, estilos de músicas, crenças, indicam e mostram seu dia a dia.

Com a chegada dos smartphones e *tablets* foi aumentando ainda mais as possibilidades de fazer parte das redes sociais e interagir com mais frequência, pois como tamanho reduzido ao se comparar com computadores, eles proporcionam a possibilidade de estar a maioria do tempo com o aparelho em mãos.

O envio e recebimento de conteúdos tornou- se muito mais rápido pois os recursos dos smartphones são inúmeros, resumindo a interação e socialização se tornoualgo rápido e fácil.

A utilização da internet é feita por meio do programa por nome de *Browser*, este de forma simples de explicar é um navegador. Basicamente ele mostra arquivos diversosda rede nas páginas de *internet*. Nessas páginas existem *hiperlinks* que possibilitam emapenas um clique a entrada em uma nova página. O *hiperlink*, ou simplesmente *link*, está em meio ao texto dentro da página, geralmente estará em cor diferente do texto (MOTA, 2012).

A cidade, lugar físico com limites bem definidos e cujo objetivo é proporcionarvida boa ao homem, agora adquire o tamanho do mundo inteiro. Diz-se que as tecnologias de informação e comunicação transformaram o mundo em uma aldeia.

O que era possível realizar localmente, em termos comunicacionais, agora pode ser feito globalmente e em tempo real. Ao mesmo tempo em que tal possibilidade se mostra vantajosa por um lado, por outro abre igualmente a possibilidade de geração deconflitos, pois é no campo da linguagem que o homem influencia e é influenciado, dominae é dominado.

Logo, pode usar as tecnologias para realizar ações benéficas, mas também maléficas, em função da ilusória sensação de anonimato proporcionado pela distância física e pela possibilidade

de se esconder atrás de um perfil falso ou *fake* (TOMAÉL, ALCARÁ; DI CHIARA 2014).

2.4 Deveres que Devem ser Seguidos em Ambiente Virtual como Fatores de Prevenção de Conflitos

Cabe aqui relembrar as palavras do filósofo grego: "a injustiça armada é a maisperigosa", e "o homem sem virtude é a mais perversa e cruel das criaturas, a mais entregueaos prazeres dos sentidos e seus desregramentos".

Aparentemente, o primeiro dos nove itens, por sua abrangência, seria suficientepara que todos os usuários da rede social em questão agissem com retidão, evitando, comoo próprio texto dispõe, infringir ou violar os direitos de terceiros ou a lei.

No sentido de auxiliar membros supostamente desavisados, o item sete é bastante importante, pois orienta aqueles que venham a ter o desejo de obter informações de outrem. Tal obtenção, diz o texto, deverá ser feita via consentimento esclarecido, ouseja, deixando claro de que forma as informações coletadas serão usadas (CONTE; FIORILLO, 2016).

De caráter didático, o item oito ensina a ter cautela quanto a publicação de dados muito visados por criminosos, como documentos de identificação ou informações financeiras. Esse dispositivo é importante e faz pleno sentido porque mesmo usuários bem instruídos e com certa maturidade costumam cometer as imprudências ali previstas,o que lhes acarreta, via de regra, sérios prejuízos financeiros ou de outra natureza (CONTE; FIORILLO, 2016).

Pode-se supor que a maioria dos usuários não lê tais termos. E mesmodesconhecendo-os, é igualmente possível supor que a maioria desses usuários possui discernimento suficiente para saber que, assim como no mundo real, é preciso respeitar o outro também no virtual.

Capez (2015, p. 136) faz uma abordagem do que em direito é conhecido comofato típico. Segundo esse autor, "fato típico é o fato material que se amolda perfeitamente aos elementos constantes do modelo previsto na lei penal". Tais elementos são: condutadolosa ou culposa; resultado (só nos crimes materiais); nexo causal (só nos crimes materiais); e tipicidade. Para a presente discussão, cabe uma análise mais atenta ao elemento denominado conduta.

Ressalte-se ainda que muitas pessoas não têm a virtude referida por Aristóteles(2007), e em nome de uma liberdade de expressão cujo sentido muitos usuários constroempor si e para si, à revelia de convenções minimamente reguladoras das interações, acabam por extrapolar limites sociais aceitáveis e invadem a privacidade alheia.

E o lado desta discussão proposto pelo item oito merece ser ressaltado. Se é verdade que as pessoas têm direito à privacidade, nem todos estão preparados para administrar uma conta pessoal na internet. Muitos problemas surgem para os usuários exatamente pela falta de habilidade para lidar com as tecnologias ou pelo mero desleixocom seus dados pessoais.

Fatos como esses levam à inevitável conclusão de que não basta aprender a operar as tecnologias em seus rudimentos para ser usuário competente delas. Sabendo que a ética não é a principal virtude de muitos usuários da rede, cabe a cada um se munir deprecauções e sistemas de segurança com vistas a dificultar invasões de privacidade e disseminação de informações que venham a comprometer a sua imagem pessoal(MALAQUIAS, 2015)

2.5 Crime Digital Fundado na Ilusão da Impunidade Causada Pela Virtualidade

Quando se fala o termo digital, se refere ao universo dos computadores. Fernandes e Oliveira (2013, p. 9) dizem que "um computador nada mais é do que uma máquina, projetada para minimizar o esforço dos seres humanos na execução de tarefas rotineiras no campo da informação". Tem como função principal fazer os processamentos de dados, ele é composto por um contíguo de *Software/Hardware*, o *Hardware* contemplaa parte física, que são alguns deles unidades eletrônicas, mecânicas magnéticas e ópticas, já o *Software* caracteriza-se ao contíguo de instruções que distribuem o funcionamentoda máquina (TAVEIRA; FERNANDES; BOTINI, 2014).

O termo "digital" decorre do modo como a informação é representada nos computadores eletrônicos, sendo toda informação é codificada com apenas dois símbolos: 0 (zero) e 1 (um). De acordo com Delai (2022), tal representação é feita através de energia elétrica. E para criar uma

representação do alfabeto formado por códigos formados pelos algarismos 0 (zero) e 1 (um) com eletricidade basta controlar o fluxo de corrente elétrica em um circuito controlando sua tensão elétrica.

Dessa maneira é possível, por exemplo, aplicar 0 volta na saída de um circuito para representar o símbolo 0 (zero) e depois trocar para 5 volts para representar o símbolo 1 (DELAI, 2022). Como zero e um são chamados dígitos, e como são usados para representar qualquer dado, computadores que utilizam tal sistema de representação são classificados como digitais.

Para compreender o significado de crimes cometidos virtualmente, é necessário primeiro estudar o significado do termo "virtual". Segundo o minidicionário Aurélio da língua portuguesa, virtual é:

> [...] Que existe como faculdade, porém sem efeito atual. 2. Suscetível de realizar-se; potencial; 3. Informe. Que é efeito de emulação ou simulação (3) de determinados objetos, situações, equipamentos, etc., por programas ou redes de computadores (ZANATTA, 2016, p. 75).

Baseando-se em Mucheroni e Martinez (2013) também oferecem um conceito para virtual. Segundo eles, o virtual é real, e o oposto do virtual é o atual. Com origem etimológica no latim, "*virtualis*" deriva de "*virtus*", que por sua vez significa "força", "potência". Mas são diversos os sentidos da palavra, sendo um deles ligado à informática, que nela ganha sentido técnico.

E "sob o ponto de vista técnico, a Internet é uma grande rede que liga um elevado número de computadores em todo o planeta por meio de cabos, satélite ou redes telefônicas" (ZANATTA, 2016, p. 19). E a internet, grande representante da virtualizada comunicação humana na contemporaneidade, é um "meio privilegiado, em virtude do seu alcance, potencial e massificação" (MUCHERONI; MARTINEZ, 2013, p. 165).

Tais definições podem suscitar em um sujeito a sensação de que tudo o que é virtual é também irreal ou ficcional, isto é, pode ser objeto de uso e usufruto a seu bel-prazer, sem consequências concretas na vida real de pessoas sobre as quais as ações virtuais recaiam.

Usuários que cometem abusos, como os previstos nos termos do tópico 5 da Declaração de Direitos e Responsabilidades do *Facebook*, e que se assemelham em teor a termos de outras redes sociais, estão na verdade incorrendo em crime, causando prejuízos a outrem. Discutir tais crimes, com ênfase no furto, é o objetivo do capítulo corrente.

2.5.1 A Prática de Crimes Digitais

A Lei 10.406/2002 institui o Código Civil Brasileiro no artigo 186, é disposto que comete ato ilícito "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral" (DUARTE, 2012, p. 138).

Segundo Capez (2015, p. 134) o crime pode ser definido como "todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para existência da coletividade e da paz". O artigo 1º do Código de Processo Penal Brasileiro, datado de 1940, dispõe que "não há crime sem lei anterior que o defina". Não há pena sem prévia cominação legal" (CAPEZ, 2015, p. 56).

Logo, crime é todo delito previsto e punível por lei penal. O termo "delito", por sua vez, é usado para designar quaisquer ações e/ou comportamentos que infrinjam uma lei já estabelecida. Portanto, é uma ação ou omissão punível pela lei penal. Voltando ao ponto de partida, delito é um crime, um ato ou omissão caracterizados por uma transgressão de uma convenção legal preestabelecida e vigente.

Capez (2015, p. 134) acrescenta que o crime pode ser conceituado sob os aspectos material e formal ou analítico, o que, para a presente discussão, possui significativa relevância. Já que o crime material "É aquele que busca estabelecer a essência do conceito, ou seja, determinar os motivos pelos quais tais atos são considerados criminosos ou não".

Já o conceito formal de crime, no entender de Capez (2015, p. 134) resulta da "Mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o

legislador descreve como tal, pouco importando o seu conteúdo".

Por fim, o crime em seu aspecto analítico, que, segundo o autor Capez (2015, p.134) "É aquele que busca, sob um prisma jurídico, estabelecer os elementos estruturais do crime. A finalidade desse enfoque é propiciar a correta e mais justa decisão sobre a infração penal e seu autor, fazendo com que o julgador ou intérprete desenvolva o seu raciocínio em etapas".

Como consequência, tais crimes têm motivado profissionais da área do direito a se especializarem no chamado direito digital. De forma simplificada, tem-se o direito digital como a área do direito que se ocupa de crimes praticados com ou sobre computadores digitais.

De acordo com Brasil (2014), a quantidade de denúncias que relacionam o *Facebook* a violações dos direitos humanos e outros crimes no Brasil, aumentou em 264,5% entre 2011 e 2012. Dentre elas, as principais em números de casos são racismo(5.021), pornografia infantil (1.969) e apologia a crimes contra a vida (1.513).

Em menor quantidade estão os *links* com conteúdo sobre maus tratos contra animais (697), homofobia (635), intolerância religiosa (494), xenofobia (376), tráfico de pessoas (233), neonazismo (186) e genocídio (181).

Neste contexto de cometimento de crime em ambiente virtual emerge uma questão importante. Um número considerável de usuários de redes sociais é de pessoas menores de dezoito anos de idade. E segundo o Art. 5º do Código Civil Brasileiro (2002), "a menoridade cessa aos dezoito anos completos, quando a pessoa fica habilitada à prática de todos os atos da vida civil" (DUARTE, 2012, p. 20).

Independentemente da idade do agente, porém, quem é vitimado tem o direito de receber os devidos reparos previstos em lei. Quanto às penalidades para crianças e adolescentes, no Brasil há disposições legais suficientes para tratar de crimes cometidos por pessoas nesta fase de sua vida.

O fato é que a prevalência da Internet criou uma nova categoria de crime — o cibercrime ou crime cibernético (SYMANTEC, 2022). Para Symantec (2022), crime cibernético é nada mais que um crime com um ingrediente "informático" ou "cibernético".

A própria *Symantec*, com base nas diferentes definições de crime cibernético, o define como qualquer delito em que tenha sido utilizado um computador, uma rede ou um dispositivo de *hardware*. Coloca ainda tais crimes em duas categorias. Tipo I e II.

Os cibercrimes do tipo I, do ponto de vista da vítima, são eventos que ocorrem geralmente uma vez. Como exemplos, são citados o *phishing*, o furto ou a manipulação de dados ou serviços através de pirataria ou vírus, furto de identidade e fraude no setor bancário ou de comércio eletrônico (SYMANTEC, 2022).

Fazem parte do Tipo II, sem ter limites às atividades como estes os de assédio e molestamento via internet, a prática de violência infantil, o ato de chantagear, realizar manipulações no mercado de valores, espionagem empresarial complexa e planejamento ou práticas de atividades terroristas. Ao contrário do Tipo I, possuem uma série contínua de acontecimentos que envolvem interações repetidas com a vítima (SYMANTEC, 2022).

A facilidade de armazenar e acessar grandes quantidades de informações em computadores tem motivado as pessoas em geral a usarem esses aparelhos para executarem tal prática. Sabedores deste fenômeno, tornou-se também crescente o interesse de agentes cujo objetivo é obter tais informações de forma ilícita, o equivalente a furto, a manipulação de dados sem consentimento do seu proprietário ou furto pode resultar em perdas significativas para pessoas físicas e/ou jurídicas.

2.6 Das Lacunas nas Legislações Existentes

A partir dos estudos apresentados, fica perceptível a ausência de legislação específica dirigida aos crimes virtuais, e registrado o interesse por parte das autoridades em criar tais leis. As dificuldades, no entanto, estão ligadas aos conflitos que as mesmas podem gerar com as leis que regem os direitos fundamentais, como a liberdade de expressão.

É dever do Direito encontrar os meios cabíveis para sanar as situações referentes aos crimes

virtuais até o momento em que seja consolidado um conjunto de leis específicas que vislumbre os mesmos. Mesmo que o ordenamento jurídico não consiga,de imediato, disponibilizar todas as ferramentas para a completa tutela dos bens jurídicos provenientes do uso da internet, é preciso proteger os interesses mais relevantes para asociedade; ou seja, o Direito deve se empenhar ao máximo para acompanhar a evoluçãoda tecnologia, no caso, e analisar cada caso concreto. Em outras palavras, mesmo não havendo uma legislação específica, o Direito tem que disponibilizar regras já existentespara proteção destes direitos (PINHEIRO, 2017).

O interesse existe, e foram mencionados, no presente estudo, projetos em tramitação, a exemplo do PL 1785/2011. Porém, para que tais projetos cheguem a vigorar,faz-se necessária sua análise minuciosa e seu cruzamento com a legislação já vigente, uma vez que o texto de um projeto que o leve a ir contra determinados preceitos legais otorna inconstitucional.

2.6.1 A Internet e o Direito Penal

Nas palavras de Pinheiro (2017) tratando sobre tipificar os crimes virtuais é deque

> "Legislar sobre a matéria de crimes na eradigital é extremamente difícil e delicado. Isso porque sem a devida redação do novo tipo penal corre-se o risco de se acabar punindoo inocente" (PINHEIRO, 2017, p.198).

O grande desafio, ao lidar com o tema, é compreender quais os bens protegidos, já que, tradicionalmente, o Direito Penal (1940) lida com a proteção de objetostangíveis. Entretanto, este panorama deve mudar rapidamente em função da importância que a informação tem no desenvolvimento da era pós-industrial.

Nas palavras de Zanatta (2016), com efeito, isto se deve, principalmente, porque na aplicação das doutrinas de direito penal tradicional a exigência da tangibilidade temsido um impedimento para punir certos crimes por computador. O Direito Penal da Informática, ao contrário, trata de conceitos intangíveis.

Não se olvide ainda, a recente publicação do diploma normativo ordinariamente achado Lei Carolina Dieckmann, que será adiante abordado de forma mais minuciosa neste trabalho. Note-se que todos os pontos enfatizados podem ensejar grandes dores decabeça aos operadores do Direito, por envolverem novos conceitos e, principalmente, oordenamento jurídico de vários países.

2.6.2 Tipos de Agentes

A maioria dos delitos que ocorrem na internet os vilões desses ataques são conhecidos por hackers, nome genérico dado aos chamados piratas de computador. "Essa expressão surgiu nos laboratórios de computação do MIT (*Massachusetts Institute of Technology*), onde estudantes passavam noites em claro averiguando tudo o que se podia fazer com um computador" (JORGE. 2018, p. 71).

Grandes empresas para proteger suas informações contratam essas pessoas para que identifiquem falhas no sistema e prestem segurança no caso de um possível ataquemalicioso. Diante disso os verdadeiros vilões do mundo cibernético são os *crackers*. Eles sim possuem um potencial poder ofensivo.

Além dessas pessoas com maiores habilidades técnicas para realizarem atos infracionais como estelionato, fraude e a invasão de dispositivo, ainda existem os usuários anônimos, mais conhecidos como *anonymous*, ou seja, são pessoas com identidades desconhecidas. Representa o conceito de muitos usuários de comunidades online existindo simultaneamente como um cérebro global.Os usuários anônimos são os que cometem a maioria dos crimes de pornografia infantil, contra a propriedade intelectual e a liberdade individual. Todas as dificuldades enfrentadas pela lei e pelas autoridades em identificar os autores dos crimes é justamente pela facilidade que o meio informática permite de mascarar a sua identidade, podendo sepassar por outras pessoas, com fim de falsificar dados para denegrir uma imagem ou aindapor pessoas anônimas para realizar atos sem serem reconhecidos.

2.6.3 Meios de Prova

No direito processo penal o que se busca é a verdade real dos fatos. O que se pretende é que o juiz e as partes tenham uma ampla liberdade para produzir provas capazes de comprovar seus argumentos. Prova é tudo aquilo que pode ser utilizado paraque se possam demonstrar os fatos alegados e perseguidos no processo (JORGE, 2018).

Aos crimes virtuais a prova pericial será requerida pelas duas partes, autor e réu, pois quando da denúncia o sujeito ofendido irá designar o perito para a comprovação dos fatos, enquanto o sujeito autor do fato requererá perito para que demonstre a sua defesa(BARRETO; BRASIL, 2016).

A perícia é o exame realizado no objeto do crime por profissionais com amplos conhecimentos técnicos, para que possam auxiliar o juiz na formação de sua convicção. O documento que atesta os dados obtidos é denominado de laudo pericial.

A prova por interrogatório é um meio pelo qual é ouvido o acusado sobre o atoa que ele está sujeito. Esta prova tem duplo sentido jurídico, pois leva o juiz ao convencimento quanto à autoria do crime, e serve também como meio de defesa da parte, quando do exercício de seu direito de contraditório e ampla defesa.

2.6.4 A Necessidade Da Regulamentação Sobre Undernet

A necessidade da regulamentação sobre *undernet* ou *Deep Web* se caracterizapor ser um meio de navegação e compartilhamento de informações mais profundas. Alguns estudos ilustram a internet como um iceberg onde a navegação é dividida em superficial, são aquelas onde todos têm acesso às informações e as mais profundas comarquivos confidenciais e sigilosos onde são difíceis de acessar e serem revelados, como por exemplo a *deep* web, aqual não possui fiscalização de conteúdo, e a criminalidadeacontece com mais facilidade.

Não se trata, propriamente, de crimes de informática, mas de crimes (comuns ou especiais), tipificados para proteger determinados bens jurídicos, em que o sistema de informática é, apenas, o meio ou o instrumento utilizado para a sua realização (SANTOS,2019).

Há uma argumentação acerca da impossibilidade de aplicação das leis penais por analogia, de forma que, apenas com a elaboração de leis específicas esta questão seria superada. Os conflitos quando da adoção da legislação por analogia e a ausência de leisespecíficas resultam na fragilidade do sistema jurídico quando se trata de crimes virtuaise, consequentemente, sua maior exploração e aumento de ocorrências.

2.6.5 Digressões sobre a Necessidade de Lei Especial para os Crimes Virtuais

É inequívoco na doutrina a dificuldade em conceituar e tipificar os crimes praticados pelo meio virtual, e o cerne da questão se encontra no artigo 1º do Código Penal brasileiro (1940), que preceitua o princípio da legalidade quando diz que não hácrime sem lei anterior que o defina. Não há pena sem prévia cominação legal.

Segundo Pinheiro (2017), todas as leis e regras sociais que existem no mundo real também devem ter eficácia no meio virtual, e é necessário estudar e criar normas específicas, mas tendo o cuidado de não fazer com que essas normas não interfiram noprincípio da liberdade de acesso e tráfego na rede.

O Estado deve promover medidas específicas para combater o crime virtual e não somente colocar a polícia atrás dos criminosos. O governo deve, paralelamente, adotar outras medidas capazes de inibir o crime e reduzir os custos da aplicação da lei penal, com distribuí-los com a sociedade.

Neste sentido, se fez necessário que houvesse uma legislação específica para tratar do assunto, buscando uma criminalização mínima, que comine penas de privação da liberdade, combinadas com multas compatíveis, prevendo penas acessórias, alternativas ou cumulativas, consistentes na imposição aos condenados de assistência programada aos órgãos de investigação, ajudando-os a prevenir e detectar fraudes e outras ilegalidade.

Para Pinheiro (2017), antes mesmo da criação da Lei Carolina Dieckmann, os especialistas da área de direito penal eletrônico afirmavam que 95% dos crimes ocorridos no meio

informático já estavam previstos, havendo necessidade de se preencher essa lacuna de 5%.

Na opinião de Santos, (2019), corrobora com a opinião de que o Código Penalbrasileiro consegue punir de 90 a 95% dos crimes praticados no meio virtual. Para concretizar sua tese, o autor cita um quadro elaborado pelo Delegacia de Repressão aos Crimes de Informática (DRCI), que enumera os crimes praticados pelo meio virtual e que já possuem previsão no Código Penal (1940) e na legislação esparsa, quais sejam: calúnia, difamação, injúria, ameaça, furto, dano, apropriação indébita, estelionato, violação ao direito autoral, pedofilia (artigo 247 da Lei 8.069/90), crimes contra a propriedade industrial (artigo 183 e seguintes da Lei 9.279/96), interceptação de comunicações de informática (artigo 10 da Lei 9.296/96) e crimes contra software (artigo 12 da Lei 9.609/98).

A criação da legislação internacional passaria pela fase de delimitação da matéria, com o cruzamento de soluções já encontradas nos diversos ordenamentos que já disciplinaram os crimes virtuais, com a fase de elaboração sendo feita por juristas desvinculados de interesses políticos.

O que pode ocorrer é a criação de novos artigos relacionados à tipificação doscrimes virtuais, e ainda o aumento da pena daqueles crimes em que o meio virtual é apenasum meio de execução (por exemplo, os crimes contra a honra). Essas alterações devemocorrer juntamente com uma alteração na Lei de Execuções Penais, alterando a forma decumprimento das penas.

2.6.6 O caso Carolina Dieckmann como um Paradigma Relevante do Direito Digital

Dentro do contexto dos crimes *cibernéticos* cometidos no Brasil, tornou-se público e notório o que vitimou a atriz de telenovelas Carolina Dieckmann. A escolha do caso da referida atriz para ser aqui descrito e comentado se deu em virtude de sua notoriedade, e para não gerar problemas de ordem ética com casos de outras vítimas reais.

2.6.6.1 Lei nº 12.737/2012 ou Lei Carolina Dieckmann

A Lei Carolina Dieckmann é como ficou conhecida a Lei Brasileira Nº12.737/2012, sancionada em 3 de dezembro de 2012. Por meio dessa lei, forampromovidas alterações no Código Penal Brasileiro, como é chamado o Decreto-Lei 2.848 de 7 de dezembro de 1940. A Lei Carolina Dieckmann tipifica os chamados delitos oucrimes informáticos (BRASIL, 2020).

Entretanto, a lei não possui relação direta com o caso da atriz. O avanço das discussões que circundam o projeto do deputado Paulo Teixeira (PT-SP) apenas coincidiu com o episódio da publicação não autorizada de fotos íntimas da atriz em maio de 2012(INFO, 2013).

Quanto ao caso em si, é sabido que no referido ano de 2012, a atriz teve sua caixa de mensagens de *e-mail* invadida e seus arquivos pessoais subtraídos. O conteúdo dos arquivos consistia de fotografias da atriz, algumas das quais a mostravam em cenas íntimas de nudez. As imagens foram publicadas à revelia do desejo da atriz, e rapidamentese espalharam pela *internet* através das redes sociais (OLIVEIRA JUNIOR, 2022). A data da publicação foi 04 de maio de 2012, num total de 36 imagens.

O objetivo da lei é inibir o criminoso de praticar o crime cibernético e punir aqueles que a transgredirem. Com a alteração, o Código Penal Brasileiro recebeu o incremento dos artigos 154-A e 154-B no Capítulo IV, em sua seção dos crimes contra ainviolabilidade dos segredos, que dispõe sobre os crimes contra a liberdade individual (OLIVEIRA JUNIOR, 2022, p. 48).

> A lei do artigo 154-A, dispõe que é crime: Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (OLIVEIRA JUNIOR, 2022, p. 57).

Por ser lei, sua completude se dá mediante penalidades previstas, a serem aplicadas aos infratores. A lei prevê como pena, aos agentes que violarem este código, detenção, de 3 (três) meses a 1 (um) ano, e multa. A pena é aumentada de um sexto a umterço caso a invasão resulte em prejuízo econômico.

3 CONSIDERAÇÕES FINAIS

É fato consolidando o avanço no uso da informática e da internet para os mais diversos fins, e é constatado que, juntamente com as facilidades e os benefícios, as ações criminosas que fazem uso das mesmas tecnologias crescem em igual proporção.

Este cenário faz premente a evolução da legislação no sentido de abordar as características destes crimes que passam a acontecer pelo meio virtual, utilizados como instrumentos de ação o computador em si, contas de e-mail, ambientes de transação, compra e venda pela internet, além de ferramentas elaboradas no intuito exclusivo de burlar a segurança digital das redes de computador.

Os fatores que promovem dificuldade estão relacionados, de forma geral, com a quebra de barreiras físicas proporcionadas pela internet, à ausência, por vezes, de provas físicas e à cautela com os direitos fundamentais do cidadão. Com o advento da *internet*, assim como é possível buscar instantaneamente informações de qualquer parte do planeta e manter contato em tempo real com pessoasigualmente distantes, também é possível cometer crimes em um território a partir de ações executadas em qualquer parte do globo, o que, por si, já caracteriza fator gerador de dificuldades, uma vez que, situações assim passam por problemas de jurisprudência.

Crimes cometidos virtualmente têm, além disto, suas ações executadas não necessariamente a partir da máquina do autor, e nem mesmo utilizando suas informações pessoais. Tal cenário concerne com a dificuldade na obtenção de provas quando a atitudeé bem pensada por parte do criminoso. Este pode cometer o crime até mesmo a partir de uma *lan house*, com utilização de dados pessoais que não os seus.

A internet permite a veiculação de qualquer tipo de informação e, muitas vezes,isso é possível mesmo sem precisar se identificar. Além de todas estas questões, ainda existe a dificuldade quando da tentativa de se estabelecer leis que regulamentem a situação, já que muitas das restrições necessárias acabariam por ferir os direitosfundamentais do cidadão. A exemplo, proibir determinados tipos de conteúdo iria contraa liberdade de expressão.

No sentido de aprofundamento, sugestões cabíveis para futuros projetos que tomem por embasamento a presente pesquisa podem ser caracterizadas pela abordagemminuciosa acerca de tipos específicos de crimes virtuais, como uma forma de aprimoraros conhecimentos acerca de cada um.

Outro tema de interessante teor seria o estudo destes direitos fundamentais docidadão que podem ser comprometidos na tentativa de se criar o tão necessárioregramento específico para os crimes virtuais. Ainda pode ser apresentada como sugestão para pesquisas futuras uma abordagem detalhada acerca das iniciativas já existentes porparte do Poder Judiciário no sentido de promover tal regramento.

A necessidade da evolução da legislação está em paralelo com a urgência da mesma, uma vez que os crimes virtuais já acontecem e são comuns. Cabe ao Poder Judiciário a iniciativa e os resultados e aos pesquisadores da área as ações e apresentações de conteúdo que contemplem o tema, em um caminho conjunto rumo à solução definitiva da situação.

REFERÊNCIAS

ARISTÓTELES. **Política**. São Paulo: Editora Martin Claret Ltda, 2007.

BARRETO, A. G. BRASIL, B. S. **Manual de investigação cibernética:** à luz do marcocivil da internet. São Paulo: Ed. Brasport, 2016.

BIROPO, B.**Computadores analógicos e digitais**. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/08/computadores-analogicos-e- digitais.html>. Acesso em: 19 abr. 2022.

BRASIL. **Constituição da República Federativa do Brasil** - 1988. 35ª edição. Biblioteca Digital da Câmara dos Deputados. Brasília: Câmara dos Deputados, 2012.

_____. **Lei nº 8.069, de 13 de julho de 1990.** Estatuto da Criança e do Adolescente. Disponível em: < http://portal.mec.gov.br/seesp/arquivos/pdf/lei8069_02.pdf>. Acesso em: 14 abr. 20222.

_____. **Decreto-lei nº 1.001, de 21 de outubro de 1969**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm>. Acesso em: 13 abr.2022.

_____. **Lei nº 12.737/2012, de 30 de novembro de 2012**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acessoem: 15 abr. 2022.

CAPEZ, F. **Curso de direito penal**. 3 ed. São Paulo: Ed. Saraiva, 2015.CARVALHO, P. R. de L..**Crimes HYPERLINK "https://jus.com.br/artigos/31282/crimes-ciberneticos-uma-nova-roupagem-para-a-criminalidade" cibernéticos: uma nova roupagem para a criminalidade.** RevistaJus Navigandi, ISSN 1518-4862, Teresina, ano 20, n. 4246, 15 fev. 2015. Disponível em: <https://jus.com.br/artigos/31282.> Acesso em: 30 set 2021.

CASSANTI, M. de O. **Crimes Virtuais, Vítimas Reais.** 2 ed. São Paulo: Ed. Brasport,2016.

CASELLI, G.; WENDT, E. **Investigação digital em fontes abertas.** São Paulo: Ed.Saraiva, 2017.

CONTE, C. P. FIORILLO, C. A. P. **Crimes no meio ambiente digital.** 3 ed. SãoPaulo: Ed. Saraiva, 2016.

CONSELHO DA EUROPA. **Convenção sobre o cibercrime**. Budapeste, Hungria.Disponível em: <http://www.acidi.gov.pt/_cfn/529350b642306/live/+Conven%C3%A7%C3%A3o+sobre+o+Cibercrime++>. Acesso em: 15 abr. 2022.

DÉLAI, A. L. **Como computadores representam informação**: representando zeros euns eletronicamente. Site eletrônico Guia do Hardware. Disponível em: <http://www.hardware.com.br/tutoriais/como-computadores-representam-informacao/representando-zeros-uns-eletronicamente.html>. Acesso em: 13 abr. 2022.

DUARTE, N. Lei 10.406 de 10 de janeiro de 2002. In: PELUSO, Cezar.**Código Civil comentado**: doutrina e jurisprudência: Lei 10.406, de 10.01.2002. Barueri, SP: Manole,2012, p.15-178.

FACEBOOK. **Declaração de Direitos e Privacidade**. Revisão 15 de novembro de 2013. Disponível em: <https://pt-br.facebook.com/legal/terms>. Acesso em: 17 abr. 2022.

FERNANDES, L. M. OLIVEIRA, R. S. **Organização de sistemas**. 3 ed. Rio deJaneiro: Senac Nacional, 2013.

FRAGA, B. **Técnicas de Invasão: Aprenda as técnicas usadas por hackers eminvasões reais.** São Paulo: Ed. Labrador, 2019.

INFO. **Lei Carolina Dieckmann entra em vigor, entenda**. Publicado em 03 de abrilde 2013. Disponível em: <http://info.abril.com.br/noticias/seguranca/lei-carolina- dieckmann-entra-em-vigor-entenda-03042013-33.shl>. Acesso em: 17 abr. 2022.

JORGE, H. V. N. **Investigação Criminal Tecnológica.** São Paulo: Ed. Brasport, 2018.

LÉVY, P. **As tecnologias da inteligência:** o futuro do pensamento na era dainformática. Trad. Carlos Irineu da Costa. Rio de Janeiro: Ed. 34, 2016.

MALAQUIAS, R. A. D. **Crime Cibernético e Prova - A Investigação Criminal emBusca da Verdade.** 2 ed. Curitiba: Ed. Juruá, 2015.

MIRABETE, J. F. FABBRINI, R. N. **Manual de Direito Penal.** Parte geral v. 1. SãoPaulo: Ed. Atlas, 2019.

MOTA, D. **Pesquisa na Internet**. Rio de Janeiro: Ed. Senac Nacional, 2012.

MUCHERONI, M. L; MARTINEZ, V. C. **Direito virtual**: breve ontologia e conceito.Tempo: Marília, SP, v. 5, p. 161-176, 2013.

NASCIMENTO, T. L. R. **Crimes Cibernéticos Conteúdo Jurídico**, Brasília-DF:Disponível em: <https://conteudojuridico.com.br/consulta/Artigos/52512/crimes- ciberneticos> Acesso em: 25 set. 2021.

NOGUEIRA, S. D. **Crimes De Informática.** 4 ed. Belo Horizonte: Ed. BH, 2018.

OLIVEIRA JÚNIOR, E. Q. **A nova lei Carolina Dieckmann**. JUS BRASIL. Disponível em: <http://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann>. Acesso em: 15 abr. 2022.

PAGANINI, P. **Os 7 crimes mais comuns no Facebook**. Disponível em: http://www.microsofttranslator.com/bv.aspx?ref=SERP&br=ro&mkt=pt-BR&dl=pt&lp=EN_PT&a=http%3a%2f%2fsecurityaffairs.co%2fwordpress%2f4891% 2fcyber-crime%2f7-most-common-facebook-crimes.html. Acesso em: 11 abr. 2022.

PINHEIRO, P. P. **Direito digital.** 6 ed. São Paulo: Ed. Saraiva Jur, 2017.

SANTOMAURO, B. **Cyberbullying**: a violência virtual. Revista Nova Escola, edição233, junho/julho de 2014. Disponível em: <http://revistaescola.abril.com.br/formacao/cyberbullying-violencia-virtual-bullying- agressao-humilhacao-567858.shtml>. Acesso em: 13 nov. 2020.

SANTOS, H. **Deep Web. Investigação no Submundo da Internet.** São Paulo: Ed.Brasport, 2019.

SANTOS, R. E. **As Teorias da Comunicação.** Da Fala à Internet. 3 ed. São Paulo: Ed.Paulinas, 2017.

SOARES, Paulo Renato. **Polícia encontra hackers que roubaram fotos de Carolina Dieckmann**. Globo.com. Fantástico. Edição do dia 13/05/2014. Disponível em: http://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram- fotos-de-carolina-dieckmann.html. Acesso em: 13 abr. 2022.

SILVA, M. A. de O. **Política**. São Paulo: Edipro, 2019.

SHIMABUKURO, A. FALCÃO JÚNIOR, A. C. G. **Crimes Cibernéticos.** Curitiba:Ed. Livraria do Advogado, 2017.

SYMANTEC. NORTON. **O que é crime cibernético?** Disponível em: <http://br.norton.com/cybercrime-definition>. Acesso em: 17 abr. 2022.

TAVEIRA, G. A.; FERNANDES, L. M. P.; BOTINI, J. **Elementos do microcomputador**. 4 ed. Rio de Janeiro: Senac Nacional, 2014.

TOMAÉL, M. I.; ALCARÁ, A. R.; DI CHIARA, I. G. **Das Redes Sociais à Inovação**.Rev. Ci. Inf., Brasília, v. 34, n. 2, p. 93-104, maio/ago. 2014. Disponível em: <http://www.scielo.br/pdf/ci/v34n2/28559.pdf>. Acesso em: 15 abr. 2022.

VIEIRA, J. L. **Crimes na Internet.**Interpretados pelos Tribunais. 3 ed. São Paulo. Ed. Edipro, 2018.

WENDT, E. **Internet e Direito Penal.** Curitiba: Ed Livraria do Advogado, 2017.

WOLOSZYN, A. L. **Vigilância & Espionagem Digital:** A Legislação Internacional e oContexto Brasileiro. Curitiba: Ed. Juruá, 2016.

WOLOSZYN, A. L.; FERNANDES, E. de O. **Terrorismo**: Complexidades, Reflexões, Legislação e Direitos Humanos. Curitiba: Ed. Juruá, 2017.

WU, T. **Impérios da comunicação:** Do telefone à internet, da AT & T ao Google. 3 ed.Rio de Janeiro: Ed. Zahar, 2016.

ZANATTA, L.**O direito digital e as implicações cíveis decorrentes das relaçõesvirtuais**. PUCRS, 2016. Disponível em: <http:/www3.pucrs.br/pucrs/files/uni/poa/**direito**/graduacao/tcc/tcc2/trabalhos2010_2/**le onardo_zanatta**.pdf>. Acesso em: 25 set. 2021.