Revista Multidisciplinar do Nordeste Mineiro, v.13, 2023
ISSN 2178-6925

CRIMINALIDADE E AS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

CRIMINALITY AND INFORMATION AND COMMUNICATION TECHNOLOGIES

Fabiana Xavier Alves, Graduanda em Direito, Faculdade Alfa Unipac de Teófilo Otoni/MG, Brasil, E-mail: fafaxavier2001 @gmail.com.

Fernanda Xavier Pereira, Graduanda em Direito, Faculdade Alfa Unipac de Teófilo Otoni/MG, Brasil, E-mail: fernandaxavierpereira1@gmail.com

Gezilan Ferreira de Souza Graduando em Direito, Faculdade Alfa Unipac de TeófiloOtoni/MG, Brasil, E-mail: Gezilan.ferreira08@gmail.com

Erica Oliveira Santos Gonçalves, Professora Orientadora, bacharel em Direito, especialista em direito processual, advogada, professora de Direito Penal e Processo Penal da Universidade Presidente Antonio Carlos - Faculdade de Direito de Teófilo Otoni/MG UNIPAC, E-mail: erica.almenara@gmail.com

RESUMO

O presente artigo, cujo tema faz abordagem à CRIMINALIDADE E AS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO tem por objetivo enfatizar a respeito dos casos que já aconteceram e vem acontecendo, bem como das leis que resguardam a problemática, objetivando as possibilidades ou impossibilidades que perduram para controlar ou evitar os crimes que são praticados através da internet, dando destaque à quais normas de proteção que devem ser tomadas para evitar os crimes, da mesma forma que as ações poderão ser utilizadas no caso de sofrer um crime dessa maneira. Esta pesquisa objetiva também, explorar o avanço do Direito Penal, frente às novas tecnologias. Com intuito de esclarecer a revolução tecnológica e seus efeitos positivos e negativos no cotidiano da sociedade; abordando diversos crimes virtuais pouco mencionados pelos doutrinadores. Porém, o Brasil atualmente não dispõe de uma legislação considerável para preservar a segurança no espaço virtual. Observando que existem dificuldades para proceder investigações em muitos casos. Entretanto, conclui-se que o Direito Penal e, consequentemente, a legislação tende a progredir para acompanhar a dinâmica social, sob pena de se tornar sem aplicabilidade aos casos concretos.

Palavras chave: Tecnologias; Crimes Virtuais; Internet;

ABSTRAT

The purpose of this article, whose theme addresses CRIMINALITY AND INFORMATION AND COMMUNICATION TECHNOLOGIES, is to emphasize the cases that have already happened and are happening, as well as the laws that protect the problem, aiming at the possibilities or impossibilities that remain to control or avoid crimes that are practiced through the Internet, highlighting which protection rules should be taken to avoid crimes, in the same way that actions can be used in the event of suffering a crime in this way. This research also aims to explore the advance of criminal law in the face of new technologies. With the aim of clarifying the technological revolution and its positive and negative effects on society's daily life; addressing various virtual crimes that are little mentioned by legal scholars. However, Brazil currently lacks considerable legislation to preserve security in the virtual space. There are difficulties in carrying out investigations in many cases. However, it can be concluded that criminal law and, consequently, legislation tends to progress in order to keep up with social dynamics, otherwise it will become inapplicable to specific cases.

Key words: Technologies; Virtual Crimes; Internet;

1. INTRODUÇÃO

Neste trabalho espira-se aclarar quanto aos crimes que acontecem no mundo virtual por intermédio da internet. Devido a percepção de impunidade que incentiva a ação de crimes virtuais. Também, especificará as dificuldades para as investigações, expondo as principais legislações acerca de tema e deliberará a diferença de liberdade de expressão e o discurso de ódio por uma sociedade usuária. Portanto, possui como objetivo principal, demostrar como acontecem os crimes cibernéticos dentro de um ambiente parcialmente novo em meio ao povo brasileiro através do espaço virtual.

Aprofundar-se a respeito da análise da evolução da tecnologia da internet no Brasil, a partir da sua origem até atualmente, considerando os crimes cibernéticos e apresentando suas principais condutas. Em seguida será explanado a prática do discurso de ódio na internet, também será abordado as legislações vigentes a respeito dessa temática. Sendo tratadas as questões ligadas ao espaço virtual, como por exemplo, o marco da liberdade de expressão, e as capacidades para combate destes crimes.

A abordagem do tema, referente aos crimes cometidos através de internet, especificamente de crime virtual, visto que, faz se a diferenciação entre alguns crimes exercidos em que o computador aponta, tal qual o significado e alcance do estudo enquanto nova modalidade do direito. O trabalho elucidará aos operadores do direito aprofundando cuidadosamente as particularidades entre os crimes já existentes e as

novas atitudes praticadas em virtude do desenvolvimento tecnológico. Assim como, demonstrar que diversos crimes praticados através de internet dispõem ideal enquadramento com paradigmas penais clássicos. Contudo, as modalidades transgressivas habituais ocorridos anteriormente ao surgimento do computador e atualmente executadas através de sua funcionalidade fomentaram as taxas de crescimento da criminalidade com celeridade e impunidade. Planeja-se potencializar compreensão sobre o moderno tema na obscura conceituação de termos tecnológicos sem moldar a essência com objetivo de transformarem desatualizados com o progresso e o complemento de novas tecnologias. A intenção deste trabalho é aguçar a reflexão quanto a celeridade do progresso tecnológico, aprofundando as particularidades desses procedimentos desenvolvidos no espaço virtual, tal como o que pode ser realizado, sobre o ponto de vista legal, para preservar os bens ameaçados.

A internet iniciou com um grande avanço no âmago da circunstancia do mundo globalizado, onde o simples acesso e a agilidade em busca de informação sendo um dos indispensáveis princípios, pois satisfaz adentrar em um site e produzir o que busca para alcançar as referências de modo célere. Considerando que ao decorrer do tempo, mais pessoas aproveitam da internet como meio de informação, para lazer, estudos, venda e compra de objetos, etc. O ambiente virtual está se transformando frequentemente na maioria dos países do mundo de forma acelerada.

Wilson Dizard diz que: “A internet é um sistema de redes de computadores interconectadas de proporções mundiais, atingindo mais de 150 países e reunindo cerca de 300 milhões de computadores”. (DIZARD, 2000).

Embora essas oportunidades e vantagens que são disponibilizadas em rede, essa conjuntura também deixa o usuário exposto a crimes, considerando que cada vez mais, criminosos utilizam desse espaço para desenvolver as mais diversificadas formas de crimes. Com o surgimento da internet em diversos lares e lugares, os crimes que já são qualificados pelo Código Penal passaram a ser executados pelo meio virtual, pois o criminoso fica “escondido através da rede”, frustrando a localização da autoria dos crimes. Sendo assim, apareceram novas modalidades de crimes que começaram a ser realizados nesse meio, despontou os chamados Crimes Cibernéticos, que embora fazerem parte da conjunção mundial e brasileira, necessita de legislação específica no ordenamento jurídico brasileiro. Mediante isso, o presente trabalho de pesquisa procura exprimir quanto o aparecimento da internet, conceito de internet, originando assim, aclarar o conceito dos crimes cibernéticos, dividindo os crimes em próprios e impróprios,

as qualificações dos crimes cibernéticos. Será abordado as legislações que concernem para os crimes cibernéticos, pesquisando a evolução histórica dos sistemas de rede e informática, e através do estudo do ordenamento jurídico examinando os instrumentos jurídicos pertinentes para moderar ou evitar os crimes cibernéticos.

2. Conceito e tipos de Crimes Cibernéticos:

2.1. Crimes Cibernéticos Puros

Crimes Cibernéticos são condutas ou atividades criminosas que abrange um computador ou dispositivo móvel com acesso à internet.

Os Cibercrimes podem ser puros ou impuros O cibercrime puro é o tipo de crime nos quais os agentes criminosos, conhecidos como hackers, muitas vezes, e crackers (do inglês "*to crack*", que significa "quebrar), precisam necessariamente de um computador ou de dispositivos móveis, eletrônicos ou informáticos para realizar ataques diretos ou remotos a computadores ou sistemas que estão protegidos, a fim de obterem bens jurídicos do sistema informático. Neste caso, não envolve apenas Intrusão massiva e captura de dados salvos com a intenção de alterar, inserir, adulterar ou destruir dados no seu computador, e sim de violar e roubar dados.

De acordo com Carneiro (2012 *apud* Viana, 2003, p. 13-26), os crimes cibernéticos puros ou ainda próprios "São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)." Também Carneiro se posiciona da seguinte forma (2012 *apud* Damásio, 2003): Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado".

Os hackers utilizam de seu profundo conhecimento técnico a cerca das tecnologias da informação para obter acesso a sistemas privados, sendo pessoa que detém conhecimento sobre o assunto e não necessariamente usa com finalidade do ato ilícito, pois desta identificação decorre que o domínio do assunto pode ser dividido em categorias positivas e negativas.

Já os crackers também chamados de *cookies* são aqueles focados em ganhos ilegais. Eles violam e desfiguram sites, não importa quais sejam, quebrar senhas e desenvolver software que possa comprometer várias máquinas simultaneamente ao

mesmo tempo. Ou seja, conceitualmente, em suma, cracker é uma espécie do gênero hacker, que não precisamente são maléficos. Inclusive, muitos hackers atualmente investigam ou participam de investigações em cibercrimes, bem como em desenvolvimento de softwares de segurança.

2.3. Crimes Cibernéticos Impuros

Crimes cibernéticos impuros ou inapropriados são aqueles cometidos por meio de um computador. Ao contrário dos crimes cibernéticos puros, esta forma de crime utiliza o computador como mero instrumento para realizá-lo. Desta forma, Carneiro (2012, *apud* Damásio, 2003) demonstra que:

> [....] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não computacionais ou diversos da informática.

Conforme essa conceituação, resta mais elucidada a concepção dos crimes cibernéticos puros e impuros; salientando-se sempre que um tipo necessariamente precisa do computador, enquanto o outro precisar do computador apenas como meio para a prática delituosa.

2.3. Espécies Mais Comuns de Crimes Cibernéticos

As espécies mais comuns de ataques, crimes cibernéticos, as quais atuam para burlar as segurança dos softwares, bem como, aproveitarem-se da ingenuidade humana, são:

2.3.1. PHISHING

Essa modalidade de ataque cuja nomenclatura origina-se do verbo “pescar” na língua inglesa, “*to fish*”, caracteriza-se pela “pesca”, por assim dizer, pela captura de informações não solicitadas estimulando a vítima, pela mensagem ou e-mail em questão, geralmente com links associados a supostas tragédias, celebridades, *reality shows* ou cobranças, entre outras, a acessar sites, conteúdos fraudulentos, sob pretexto de estes serem governamentais, bancários ou de empresas respeitadas. Atualmente, essa palavra também designa a forma de cibercrime de envio de informações para criminosos.

2.3.2. RANSOMWARE

O *ransomware*, de “*ransom*” (“valor pago” ou “resgate para sequestro”, em inglês) com “*malware*” (malicioupor sua vez composta pela junção de “*malicious*” com “software”), por sua vez, caracteriza-se por uma modalidade de ataque cibernético que objetiva conseguir dinheiro das vítimas, muitas vezes, por *bitcoins*, uma moeda eletrônica universal, não subordinada a um governo ou país específico, por bloquear a tela do computador exibindo a notificação para que seja feito o pagamento, tão como, mais atualmente, criptografar todo o dispositivo em questão.

Geralmente os *ransomwares* manifestam-se mediante mensagens de *phishing*, e por sites e contas em redes sociais que, sim, são éticas, famosas e seguras, mas que foram hackeadas. A proposta apresentada no PL 879/2022 indica pena de três a seis anos de prisão, além de multa, para os cibercriminosos que invadirem dispositivos e redes para bloquear arquivos.

A punição aumenta para até oito anos de reclusão caso seja cobrado resgate para devolução das informações. Quanto às penalidades, existe artigo 154-A do Código Penal, § 1º, que assim tipifica, consoante a seguinte transcrição:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

Bem como se aplica, nesta situação pela extorsão, o artigo do mesmo Diploma Legal, nos seguintes termos:

> Art. 158 – Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa:
> *Pena – reclusão, de quatro a dez anos, e multa.*

> Para um escopo mais preciso e particular do *ransomware*, existe o Projeto de Lei (PL) 879 de 2022, do senador Carlos Viana, que indica a pena de três a seis anos de prisão, além da

> multa, em casos de cibercriminosos que invadam dispositivos e redes para bloquear arquivos. A punição aumenta para até oito anos de reclusão se for cobrada a devolução ou resgate das informações.

Como precedente do ransomware no brasil deu-se o paradigma jurídico da lei Carolina Carolina Dieckmann.

A Lei N. º 12.737 de 2013, popularmente conhecida como Lei Carolina Dieckmann, deu-se como sancionada, em 30 de novembro de 2012, à causa de que se criasse uma legislação acurada e específica para situações de estorções, subtração e ou manipulação de dados mediante as tecnologias da informação. O antecedente criminal para que isso acontecesse foi a violência a esse mesmo respeito de dados de si mesma, mais precisamente fotos se conteúdo íntimo e sexual, que a atriz Carolina Dieckmann sofreu.

Nessa toada, resumida e mais detalhadamente, ocorreu que um grupo pequeno e independente de hackers, ou ciberpiratas, pessoas com profunda expertise da computação e da informática, quem trabalham a desenvolver e a modificar hardwers, vem como softwares e hardwares de diversas redes e dispositovos, não necessariamente para malfazerem alguma prática criminosa, invadiram o computador pessoal da atriz para invadir, e com sucesso, e, em seguida, divulgar sem autorização trinta e seis fotografias libidinosamente reveladoras, as quais eram, por sinal, para seu marido, nas redes sociais e páginas pornográficas. Em continuidade, além dessas fotografias saqueadas, a atriz foi ameaçada e extorquida para que não houvesse a exposição. A Carolina Dieckmann negou-se ceder à chantagem, e teve aquelas suas fotografias publicadas.

Situacionalmente, não tardou, diante de tal escândalo de gênero inédito em tamanha proporção, o caso dessa ação na Justiça, impetrada pela atriz, rapidamente ganhou a notoriedade.

2.3.3. PORNOGRAFIA INFANTIL

A pornografia infantil é uma modalidade de cibercrime sumamente desumana, em termos de ética, e estruturada mente difundida. Existem quadrilhas internacionais e multimilionárias que se sustentam financeiramente da pornografia infantil. Essa modalidade de crime virtual é sumamente difícil de ser descoberta. Porque os agentes, muitas vezes, detêm grande conhecimento de informática, ganham muito dinheiro e não atuam sozinhos; trata-se de uma rede milionária e muito discreta. A INTERPOL, a Polícia

Internacional, é a principal instituição mundial a combater a pornografia infantil. O ECA – Estatuto da Criança e do Adolescente — Lei n. º 8.069, de 13 de julho de 1990, previa pena de 1 a 6 anos; infra é, pois, a transcrição dessa legislação.

> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
>
> § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
>
> § 2o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por: (Incluído pela Lei nº 11.829, de 2008)
>
> I – agente público no exercício de suas funções; (Incluído pela Lei nº 11.829, de 2008)
>
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo; (Incluído pela Lei nº 11.829, de 2008)
>
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. (Incluído pela Lei nº 11.829, de 2008)
>
> § 3º As pessoas referidas no § 2o deste artigo deverão manter sob sigilo o material ilícito referido.

Com o Projeto de Lei (PL) 830 de 2022 de Flávio Bolsonaro, sob a prática de registrar, vender ou expor pornografia infantil recai-se a pena de 5 a 8 anos de reclusão e multa; sob divulgar material pornográfico infantil tem-se a pena de 4 a 6 anos de reclusão e multa; por armazenar registro pornográfico infantil recai-se a pena de 2 a 5 anos de reclusão e multa, ressalvando-se que não é configurada crime a guarda e a posse da pornografia para comunicar às autoridades a ocorrência do crime, desde que a comunicação seja feita pelos indicados nos artigos arts. 240, 241, 241-A e 241-C do ECA, e, também, ressalva-se que se o material pornográfico adquirido ou guardado for de pequena quantidade, a pena pode ser diminuída de 1 a 2/3; e, por fim, sob assediar ou simular a participação infantil em pornografia é de 2 a 4 anos de reclusão e multa.

2.3.4. CYBERBULLYING

O cyberbullying é o mesmo que o bullying, porém praticado virtualmente. Isto é, é o bullying na internet. As consequências do cyberbullying podem ser tão devastadoras quanto as do bullying em situações presenciais. Ou seja, fazem tão mal à vítima quanto,

mesmo porque na internet os insultos e a perseguição se espalham muito mais rapidamente.

O cyberbullying recebe punição por parte do Código Penal quando por se tratar de crimes contra a honra; quais sejam calúnia, difamação e injúria. As penas previstas podem chegar a quatro anos de reclusão, bem como cabe a indenizações a título de dano moral.

2.3.4. DEEPWEB

Em 1980 um funcionário da CERN (Organização Europeia para aInvestigação Nuclear), de Tim Berners-Lee desenvolveu um sistema capaz de reconhecer e armazenar inúmeras informações, no que se deu a criação do WWW (World Wide Web).

Ao longo dos anos, Michael K Bergman desenvolveu o browser (navegador) que pode ser usado para "surfar" nas redes, disponibilizando o artigo The Deep Web Surfacing Hidden Value (A rede profunda: questões referentes, valores escondidos), fazendo com que o artigo tornasse a origem à palavra Deep Web. De acordo palavras do Borges, Sartori e Barros (2015):

> A Deep Web é o conjunto de conteúdos da internet não acessível diretamente por sites de busca. Isso inclui, por exemplo e em regra, documentos hospedados dentro de sites que exigem login e senha. Sua origem e sua proposta original são legítimas. Afinal, nem todo material deve ser acessado por qualquer usuário (pode ficar dentro de sites comuns, na forma de arquivos e dados baixáveis, ou escondidos em endereços excluídos propositadamente dos mecanismos de busca).

Na Internet, pode ser determinada a localização de qualquer dispositivo desde que esteja acessado à rede, através do IP (Internet Protocol), ou seja, o IP é uma ferramenta exclusiva que computadores ou servidores tem para ser ingressado através da internet ou redes. Na Deep Web em diversos casos não é possível localizar o Internet Protocol do usuário, por existir páginas, que dificultam a localização dos usuários.

O uso da Deep Web permite que as entidades criminosas usem da rede de computadores para dividir com outros e armazenar arquivos confidenciais e que não devem estar disponíveis na internet, através da mesma é possível verificar o local, o tamanho e o tempo dos dados informados, e assim podendo deduzir quem está

comunicando com quem, por meio de um aplicativo específico, o TOR (The Onion). Borges, Sartori e Barros (2015), também explicam que:

> Ao contrário do que muitos podem imaginar, acessar a Deep Web não é ilegal. Motivados pela privacidade que o local pode proporcionar, várias pessoas recorrem à "internet invisível" para tratar de assuntos sigilosos e compartilhar arquivos que jamais poderiam "ver à luz do dia". No entanto, a condição de anonimato (o que é vedado pela Constituição Federal), dessa gigantesca parte da Internet também acaba levando ao surgimento de uma série de atividades ilegais, muitas das quais os órgãos competentes ainda têm muita dificuldade em tratar.

3. CRIMES CONTRA A HONRA

Os crimes contra a honra são tipificados no direito penal e se referem a condutas que atingem a reputação, a dignidade ou a imagem de uma pessoa. Geralmente, eles envolvem a difamação, a calúnia e a injúria. Esses crimes estão previstos no Código Penal brasileiro, mas as leis podem variar de acordo com o país.

Difamação: A difamação ocorre quando alguém atribui a outra pessoa um fato ofensivo à sua reputação, expondo-a ao desprezo público. É necessário que a afirmação seja falsa, pois, se for verdadeira, constitui uma excludente de ilicitude. A difamação pode ocorrer de forma oral, escrita ou gestual.

Calúnia: A calúnia envolve a imputação falsa de um crime a alguém, com o objetivo de causar-lhe dano à reputação. Diferentemente da difamação, a calúnia se refere a crimes específicos e não apenas a fatos ofensivos. Para configurar calúnia, é necessário que a imputação seja falsa e que o acusado saiba de sua falsidade.

Injúria: A injúria é o crime que consiste em ofender a dignidade ou o decoro de alguém, atingindo sua honra subjetiva. Geralmente, a injúria ocorre por meio de palavras, gestos ou escritos que desvalorizam a vítima. Diferentemente da difamação e da calúnia, a injúria não envolve a imputação de fatos, mas sim a ofensa direta à pessoa.

Em todos esses crimes, é necessário que a conduta seja dolosa, ou seja, que exista a intenção de difamar, caluniar ou injuriar. Além disso, é necessário que a ofensa seja dirigida a uma pessoa determinada, ou seja, que seja possível identificar quem é o sujeito passivo do crime.

No Brasil, os crimes contra a honra são considerados infrações penais de menor potencial ofensivo, o que significa que, em geral, são processados no âmbito dos

Juizados Especiais Criminais. As penas previstas para esses crimes podem variar, mas geralmente envolvem pagamento de multa, prestação de serviços à comunidade ou pena restritiva de direitos.

É importante ressaltar que a liberdade de expressão é um direito fundamental, mas não é absoluta. Ela deve ser exercida com responsabilidade, respeitando os limites estabelecidos pela legislação, para evitar abusos que atinjam a honra de terceiros.

3. DAS CONSIDERAÇÕES FINAIS

Ante toda a recente, em termos históricos e, mais precisamente, contemporâneos, problemática dos crimes cibernéticos, sabe-se à medida que as tecnologias da informação se expandem, mais, assaz possivelmente, se legislará acerca da temática, tópico. Assim é uma vez que as mazelas e dilemas virtuais apenas refletem as dificuldades e deficiências éticas e morais dos seres humanos. Desta feita e nesse sentido, por parcela significativa da população, sabendo-se disso inclusive pela sabedoria popular, ainda ser analfabeta funcional em questão, matéria de informática, os cuidados com dados nas redes sociais ante as fraudes e delitos são sumamente cruciais e demasiadamente importantes para a vida civil das pessoas. Porque, acessando, sem total conhecimento, uma ferramenta que reflete as sombras e as maldades humanas, uma pessoa, a depender do conteúdo que acessa, ser alvo fácil de golpes.

Pois bem nessa lida, assim sendo, portanto, paralelamente, disseminando-se as tecnologias da informação ao passo que a sociedade também avança em marcos tecnológicos, tais como, a exemplo, as constantes atualizações e modernidades envolvendo dispositivos celulares, mais a sociedade se reitera de quão, cada vez mais, as falcatruas estão sofisticadas e subliminares. Ora, se pressupondo-se hermenêutica e juridicamente que onde houverem relações humanas viabiliza-se que se haja o Direito, na internet, na e pela qual diversas coisas podem ser resolvidas ou problematizadas a partir de apenas um clique, tão breve, mas tão significativo quanto, essa presença judiciária faz-se necessária mais do que nunca. Afinal, pois, sendo que depois da pandemia da COVID-19 muitas empresas ainda trabalham pela modalidade de trabalho remoto, a internet veio à sociedade para ficar em todos os âmbitos, enfatizando-se e sutilizando-se mais e mais. Quem sabe assim, para arrematar, com a presença e maior atuação efetiva da Lei sobre a vivência cibernética torne o mundo um lugar mais justo para se viver.

4. REFERÊNCIAS

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. In: Âmbito Jurídico, Rio Grande, XV, n. 99, abr 2012. Disponível em: <http://www.ambitojuridico.com.br/site/n_link=revista_artigos_leitura&artigo_id=11529>. Acesso em: ago. 2023.

BORGES, SARTORI E BARROS. Daniela Cristin, Liane Pioner, Mauricio Sebastião. **A Deep Web e a relação com a criminalidade na internet**. Disponível em:> http://direitoeti.com.br/artigos/a-deep-web-e-a-relacao-com-a-criminalidade-nainternet/ Acesso: agosto. 2023.

DIZARD Jr., Wilson. A **nova mídia: a comunicação de massa na era da informação**. Rio de Janeiro : Jorge Zahar Ed., 2000.

VIANNA, Túlio Lima. **Dos crimes pela internet**. Disponível em: <http://www.academia.edu/1911162/Dos_crimes_pela_internet>. Acesso em: ago. 2023.

PORTELA, Raíssa. Senado Notícias. **Projeto aumenta pena para registro, venda e exposição de pornografia infantil**. 06 jun. 2022. [s.d.]. Disponível em: <https://www12.senado.leg.br/noticias/materias/2022/06/06/projeto-aumenta-pena-para-registro-venda-e-exposicao-de-pornografia-infantil>. Acesso em: ago. 2023.

TJDFT — Tribunal de Justiça do Distrito Federal e dos Territórios. **Adquirir Pornografia Infantil**. [s.d.]. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/adquirir-pornografia-infantil>. Acesso em: ago. 2023.

TJDFT — Tribunal de Justiça do Distrito Federal e dos Territórios. **Divulgação de Pornografia Infantil**. [s.d.]. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/divulgacao-de-pornografia-infantil>. Acesso em: ago. 2023.

Crime cibernético: entenda o que são, tipos e como se proteger. CNX Blog Conexão Algar Telecom. 16 nov. 2022. [s.d.]. Disponível em: <https://blog.algartelecom.com.br/tecnologia/crimes-ciberneticos/#:~:text=Em%20resumo%2C%20s%C3%A3o%20considerados%20cibercrimes,de%20dados%20para%20espionagem%20industrial.>. Acesso em: ago. 2023.