UNIVERSIDADE CESUMAR - UNICESUMAR
CENTRO DE CIÊNCIAS HUMANAS E SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM DIREITO

O AUMENTO DE CRIMES CIBERNÉTICOS DURANTE A PANDEMIA

JOÃO PEDRO TIVO SILVA

MARINGÁ – PR
2022

João Pedro Tivo Silva

O AUMENTO DE CRIMES CIBERNÉTICOS DURANTE A PANDEMIA

Artigo apresentado ao Curso de Graduação em Direito da Universidade Cesumar – UNICESUMAR como requisito parcial para a obtenção do título de Bacharel (a) em Direito, sob a orientação do Prof. Me. Marllon Beraldo

MARINGÁ – PR

2022

FOLHA DE APROVAÇÃO

JOÃO PEDRO TIVO SILVA

O AUMENTO DE CRIMES CIBERNÉTICOS DURANTE A PANDEMIA

Artigo apresentado ao Curso de Graduação em Direito da Universidade Cesumar – UNICESUMAR como requisito parcial para a obtenção do título de Bacharel (a) em Direito, sob a orientação do Prof. Me. Marllon Beraldo.

Aprovado em: ____ de _____ de _____.

BANCA EXAMINADORA

_____

Nome do professor – (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

O AUMENTO DE CRIMES CIBERNÉTICOS DURANTE A PANDEMIA

João Pedro Tivo Silva

RESUMO

O presente trabalho traz o desenvolvimento de um estudo sobre os crimes digitais, também conhecidos como crimes cibernéticos. A compreensão analítica do tema adentrou no mérito do amparo legal que o judiciário brasileiro dá aos crimes realizados tendo como instrumento os meios digitais, abordando inicialmente o aspecto legal dos crimes em geral, como são divididos dentro do sistema penal, como ocorrem as suas respectivas configurações e quais as penas previstas para cada tipo penal. Estudou-se então o instituto da tecnologia, e como ela se desenvolveu ao longo da história, com a criação do computador e da rede internacional da internet, compreendendo-se as mudanças sociais que acompanharam o desenvolvimento tecnológico, com alterações diretas nos hábitos de comunicação e relações sociais entre os indivíduos. O presente trabalho expõe um pequeno histórico sobre o desenvolvimento da rede mundial de internet, o que são os crimes virtuais e suas classificações, a evolução histórica e legislativa dos crimes cibernéticos, destacando a legislação brasileira durante o período de pandemia de Covid-19. O estudo amparou os reflexos sociais que os crimes digitais promovem, trazendo à baila os aspectos econômicos e políticos correlacionados ao tema, compreendendo também as consequências jurídicas possíveis para penalização dos criminosos e as buscas pela otimização no plano da prevenção a novos casos. Compreendeu-se ao término do estudo que a internet é um instituto que toma cada vez mais espaço no mundo, com a otimização das relações sociais e de trabalho, mas também abre caminho para a ocorrência de diversos tipos de crimes que precisam cada vez mais do amparo e atenção do poder judiciário e legislativo para que as consequências sejam tomadas em relação aos criminosos.

Palavras-chave: Crimes. Internet. Direito. Penal.

THE RISE OF CYBER CRIME DURING THE PANDEMIC

ABSTRACT

This work brings the development of a study on digital crimes, also known as cyber crimes. The analytical understanding of the subject went into the merits of the legal support that the Brazilian judiciary gives to crimes carried out using digital media as an instrument, initially addressing the legal aspect of crimes in general, how they are divided within the penal system, how their respective configurations occur. and what penalties are foreseen for each type of penalty. The institute of technology was then studied, and how it developed throughout history, with the creation of the computer and the international internet network, understanding the social changes that accompanied technological development, with direct changes in communication habits and social relationships between individuals. The study then proceeded to pay attention to crimes committed digitally, and how they can be typified and correctly identified so that it is possible to

apply penalties and accountability for the individual who commits criminal acts through the internet. still, the study supported the social reflexes that digital crimes promote, bringing to light the economic and political aspects related to the theme, also understanding the possible legal consequences for penalizing criminals and the search for optimization in the prevention of new cases. It was understood at the end of the study that the internet is an institute that is taking more and more space in the world, with the optimization of social and work relations, but also opens the way for the occurrence of different types of crimes that need more and more attention. support and attention from the judiciary and the legislature so that the consequences are taken in relation to criminals.

Keywords: Crimes. Internet. Criminal. Law.

1. INTRODUÇÃO

Quando se estuda a influência da tecnologia para o Direito Penal se percebe que, para o ordenamento jurídico como um todo, este é um assunto bastante moderno, tendo em conta a opinião de maioria dos doutrinadores de que não existem leis que sejam suficientes para dissolver as divergências de todas as áreas oriundas do avanço da tecnologia.

Ademais, também pesam as dificuldades na investigação penal, tendo em conta que, ainda que seja possível averiguar os responsáveis por determinado delito virtual, ainda há uma carência tanto em recursos para tanto, quanto de profissionais que possuam o conhecimento técnico necessário para lançar mãos de tais recursos, gerando uma sensação de impunidade.

A impunidade, além disso, faz com que as vítimas, em grande parte dos casos, acabem desistindo de denunciar o que sofreu às autoridades, ignorando os danos sofridos ou buscando resolvê-los e repará-los por outros meios.

Desta forma, o presente artigo visa analisar alguns dos principais delitos e os bens jurídicos tutelados pelo Direito Penal que se encontram ameaçados pelas mudanças tecnológicas. Ademais, será analisado, de modo paralelo, alguns dos princípios constitucionais que se coadunam com o assunto, de maneira que se compreenda os estudos de doutrinadores e as soluções destes para os conflitos relacionados à tecnologia.

Recentemente com o surgimento da pandemia do novo coronavírus, uma das medidas mais adotadas ao redor do mundo foi o isolamento social, e a adesão ao trabalho remoto visando diminuir ou evitar aglomerações nos espaços de trabalho e ou até ver familiares e amigos. Com isso acabou tendo um aumento gigantesco de aparelhos informáticos conectados simultaneamente, o que acabou por favorecer ainda mais a prática deste tipo de delito. E esse espaço virtual de comunicação instantânea entre pessoas em diferentes pontos no mundo, torna-se o lugar perfeito para prática de diversos tipos de delitos realizados através dos aparelhos informáticos.

O tema disposto é bastante atual relevante, pois mostra como os crimes virtuais vem crescendo e se diversificando na sociedade. E mesmo que o ambiente virtual transmita a sensação de terra de ninguém ou terra sem lei, em possíveis situações em que o crime virtual ocorra e seja devidamente comprovado, os perpetradores devem ser responsabilizados de acordo

2. CONCEITO DO CRIME CIBERNÉTICO E SUAS PRINCIPAIS CARACTERÍSTICAS

O desenvolvimento humano, ao longo da história, foi movido pelo desbravamento da natureza e busca por melhorias na qualidade de vida, assim, a história do crescimento em massa e mudança nos conhecimentos de produção chegou até a revolução industrial, e começou a dar passos cada vez mais rápidos rumo a um crescimento tecnológico grandioso.

A compreensão da tecnologia como uma aliada ao desenvolvimento social e econômico foi ganhando forma na medida em que o globo inteiro era apresentado aos inventos que eram produzidos com a união da evolução da ciência e da tecnologia, que dava possibilidades de melhorias nas atividades mais corriqueiras da vida humana.

Na época da revolução industrial, o trabalho humano foi transformado com as diversas possibilidades que as invenções de maquinários foram surgindo, trazendo a produção de mais produtos e em uma escala nunca antes vista.

O estudo do fenômeno social que acontecia junto com a evolução tecnológica é importante quando se tenta entender como o poder legislativo e judiciário vão ganhando espaço e aplicabilidade no contexto social em que estão sendo imergidos. O entendimento dos conceitos e a abordagem desses entendimentos quando à conduta das pessoas é essencial para que sejam efetivas as medidas de amparo estatal aos indivíduos que precisam de sua tutela.

A integração dos frutos do processo de desenvolvimento tecnológico com a rotina das pessoas na sociedade, foi acontecendo gradualmente, porém numa constância que fez com o crescimento da demanda por maquinários residenciais gerasse mais incentivo à criação de instrumentos que facilitassem a rotina doméstica e o trabalho.

A tecnologia foi ganhando cada vez mais espaço, tendo passado de uma aliada do setor industrial e do crescimento exponencial da produção para uma forma de facilitação doméstica, e, então, para interferir no ambiente de trabalho com a ingerência dos benefícios que causava à produtividade.

A busca, por exemplo, das facilitações no ramo do cálculo, sempre existiu, e no século XVII surgiu uma mudança positiva nesse panorama com a criação da primeira calculadora, por Pascal[1].

---

[1] [...] Blaise Pascal (1623-1662) foi um físico, matemático, filósofo e teólogo francês. Autor da famosa frase: "O coração tem razões que a própria razão desconhece". [...]FRAZÃO, Dilva. Blaise Pascal Filósofo francês: biografia de blaise pascal. **Ebiografia**, [*S. l.*], p. 1-2, s/d. Disponível em: https://www.ebiografia.com/blaise_pascal/. Acesso em:

As descobertas científicas e invenções tecnológicas foram, então, crescendo num processo evolutivo que, a cada aprimoramento, como visto acima, trazia melhorias e mais possibilidades para com o produto final gerado.

O período compreendido pelo século XX, em especial a sua primeira metade, foi marcado pelo desenvolvimento tecnológico ligado à computação, mais especificamente aos computadores mecânicos, e, com a chegada da segunda grande guerra, houve ainda mais necessidade de uso do desenvolvimento tecnológico dos computadores, ainda mais com a necessidade de desencriptação de mensagens, como reflete Gugik:

> A Segunda Guerra Mundial foi um grande incentivo no desenvolvimento de computadores, visto que as máquinas estavam se tornando mais úteis em tarefas de desencriptação de mensagens inimigas e criação de novas armas mais inteligentes. Entre os projetos desenvolvidos nesse período, o que mais se destacou foi o Mark I, no ano de 1944, criado pela Universidade de Harvard (EUA), e o Colossus, em 1946, criado por Allan Turing. Sendo uma das figuras mais importantes da computação, Allan Turing focou sua pesquisa na descoberta de problemas formais e práticos que poderiam ser resolvidos através de computadores. Para aqueles que apresentavam solução, foi criada a famosa teoria da "Máquina de Turing", que, através de um número finito de operações, resolvia problemas computacionais de diversas ordens. A máquina de Turing foi colocada em prática através do computador Colosssus, citado acima.[2]

A análise da importância da evolução da computação no período da guerra é de grande relevância quando se reflete a respeito da ligação entre o desenvolvimento tecnológico e as suas ingerências no plano social e político, e a necessidade de que seja amparado pelo poder legislativo na medida em que muda o cenário que atinge.

2.1 CRIMES DIGITAIS

A abordagem dos crimes digitais no setor do judiciário é coligada ao panorama que a tecnologia estabeleceu ao longo dos anos, com o advento dos computadores, e da internet, fatores que trouxeram grandes mudanças na comunicação da sociedade, que a atingiram a nível global.

A necessidade de um amparo judicial que sustentasse o advento de um novo e revolucionário tipo de interação social é clara quando se analisa que a sociedade como um

[2]GUGIK, Gabriel. A história dos computadores e da computação. **Tecmundo**, [*S. l.*], p. 1-5, 6 mar. 2009. Disponível em: https://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm. Acesso em:

todo está sujeita a utilização das ferramentas digitais na rotina, e isso pode causar diversos tipos de atrito entre os usuários, que refletem na vida fora das telas na medida em que refletem uma realidade que existe apesar da rede.

O judiciário tem o dever de amparar as situações jurídicas que se instalam a nível social, já que cabe a ele dirimir os conflitos interpessoais no panorama dos direitos, deveres e sanções, assim, a criação de dispositivos legais que mostrem as possibilidades de cometimento de crime no âmbito digital é essencial para que haja amparo das pessoas que estão sujeitas a sofrerem as consequências da conduta online de outrem, e para evitar que os crimes sejam replicados, especialmente pelo verdadeiro banco de dados do qual se compõe a rede que forma a internet.

O surgimento da internet impactou diretamente as relações sociais, trazendo mudanças drásticas que tanto afetam as pessoas quanto o sistema em si, que se viu cada vez mais imerso no universo que era apresentado pela internet, tanto tendo que se encaixar em sua formação, integrando-se cada vez mais à rede, quanto na percepção de como a conduta das pessoas afetava o sistema como um todo.

Assim a informática aliou-se ao mundo de tal forma que a sua integração com as pessoas tem um fim que vai além da mera comunicação, e repousa os interesses na vivência social, na rotina das pessoas, trazendo um teor de essencialidade na medida em que sempre se está cercado dos benefícios e da carga informativa trazidos pela internet.

A tecnologia, aliada à internet, promove inúmeros benefícios à populações ao redor do mundo, com a difusão de conhecimento e informação e troca de experiências, diminuindo as distâncias e possibilitando mais e mais desenvolvimento tecnológico que resultam até mesmo em benefícios para a saúde humana, além das melhorias no transporte, educação e até mesmo geração de empregos.

A grande questão que envolve o lado ruim dos adventos tecnológicos mora na ideia que a internet é um universo inteiro que existe em paralelo à realidade social, pensamento este que se instaurou por algum tempo, trazendo a percepção de que não se aplicava ao campo digital o que se compreendia pessoalmente. Assim, a prática de diversas atividades digitais, mesmo as que trouxessem prejuízos a terceiros, foi compreendida como não passível de penalização.

A existência de lacunas na lei tem um potencial muito grande de esconder as práticas ilícitas das penalidades que deveriam existir caso fossem verificadas que as consequências traziam ou poderiam trazer prejuízo a um terceiro.

A sociedade, com os adventos tecnológicos tão avançados, se mostra, com o advento de uma sociedade digital, passível de ser um alvo da criminalização digital quando não tem uma regulação que sustente as possibilidades de crimes online, e as consequências das práticas criminosas.

O Direito, como tem o dever de caminhar ao lado da sociedade, acompanhando as mudanças que ocorrem em cada época com os indivíduos e resguardando os direitos destes, tem que enxergar na vivência social online as possibilidades criminais que existem, e amparar os usuários.

A internet não só representa, no quadro social atual, uma forma de haver desenvolvimento nas tecnologias de comunicação e disseminação de informação, sendo também uma forma de geração de dinheiro, na medida em que o trabalho online, e a transformação dos meios de vendas de produto com a existência de um comércio eletrônico, trazem uma importância econômica muito grande para o Estado.

A necessidade de organização dos meios virtuais de acordo com uma legislação que regule as possibilidades desse meio vem tanto da possibilidade de práticas que tragam inúmeros prejuízos para os usuários, com a prática de crimes online, bem como da possibilidade de prática comercial que necessite de uma regulação tributária.

O que se entende nesse panorama é que o amparo legal é essencial para uma regulação do que se traz na internet. A respeito do assunto, Crespo:

> Dessa forma, naturalmente surgem inquietações dos homens quanto a leis que venham a regular o desenvolvimento tecnológico. Isto porque o avanço das tecnologias impõe complexos problemas jurídicos a serem decifrados pelos operadores do direito. Com a interação cada vez mais intensa de informática e direito, a análise dos problemas jurídicos levantados pelos computadores ficaria a cargo do Direito da Informática. Por outro lado, num sentido diametralmente oposto, podemos denominar de informática jurídica a penetração da informática no universo jurídico. A doutrina define a informática jurídica como o ramo da informática que compreende as suas aplicações específicas ao mundo do direito, complementando o trabalho daqueles que operam com o direito através do processamento e armazenamento eletrônico de informações jurídicas. Em outras palavras, trata-se do estudo da aplicação da informática como instrumento, e o consequente impacto na produtividade dos profissionais do Direito.[3]

[3]CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1. ed. São Paulo: Saraiva, 2011. 70 p. ISBN 9788502136663. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=Px9nDwAAQBAJ&oi=fnd&pg=PT8&dq=crimes+digitais+e+redes+sociais&ots=8aAv_oj9JJ&sig=InmRJoKo8dByJTOoW7cyAV4NsKw#v=onepage&q=crimes%20digitais%20e%20redes%20sociais&f=false. Acesso em:

O autor continua a reflexão trazendo como o direito da informática tem a sua definição amparada pelo judiciário:

> Já o direito da informática é definido como o ramo do direito que delineia, estuda e busca resolver os problemas jurídicos advindos da evolução tecnológica, ou, nas palavras de Marques e Martins, trata-se da análise e resolução do complexo de problemas jurídicos levantados pelo computador. De fato, o direito da informática não parece ser, ao menos até agora, um ramo específico do direito. Soa, assim, muito mais algo como uma releitura, uma reinterpretação das normas jurídicas à luz da sociedade da informação que propriamente um novo ramo.[4]

Compreende-se então, que a interação do direito com o meio digital é pautada tanto na correlação entre o judiciário e a rede (através dos processos virtuais, jurisprudência pátria, doutrina e legislação), quanto na necessidade de que os fenômenos sociais que acontecem na internet e tem uma repercussão nesta ou na sociedade como um todo, sejam amparados por regulamentação legal que responsabilize os sujeitos que cometem ações online.

A compreensão da prática é que ela é basicamente um tipo de fraude que enseja ao roubo de informações, seja de pessoas físicas ou jurídicas, com o intuito de usar essas informações para conseguir efetuar transações online com os dados da pessoa lesada.

Crime de pedofilia, sem dúvida figura como possivelmente o pior deles, pois agride a integridade de crianças e jovens que deveriam ser absolutamente protegidos dos criminosos que cometem as ações terríveis que levam à configuração dos crimes relacionados à pedofilia.

Olhando sob o panorama do judiciário brasileiro, compreende-se que a pedofilia abrange o crime de pornografia infantil, além de abuso infantil, sendo o crime mais visto no que se trata da pornografia infantil. Assim houve uma otimização no Estatuto da Criança e do Adolescente no sentido de trazer ainda mais evidente a luta contra a pornografia infantil, tanto na venda quanto na produção da mesma.

Existem ainda os crimes contra a honra, como: calúnia, que é compreendida no rol de crimes contra a honra por configurar a atribuição da autoria de um crime a outrem, sendo que essa fala para terceiro seja feita de forma pública, com a exclamação de que alguém cometeu um crime em uma via de visualização possível por um número de pessoas.

A internet traz a possibilidade de ser lugar para um crime de calúnia pois a interação social é generalizada, e com isso, espalhar de forma caluniosa a autoria de um crime pela internet é crime. A tipificação legal está prevista no Código Penal brasileiro, em seu art. 138; crime de injúria, figura no Código penal em seu art. 140, e é um tipo criminal que traz uma

[4] Ibid., p. 22

ofensa à honra pessoal da vítima, não sendo necessário que haja a presença ou ciência de terceiro para que seja configurado, como ocorre no caso acima compreendido; crime de difamação, que ocorre quando alguém imputa a outrem algum fato que compromete a reputação deste. Diferentemente dos casos de calúnia, na difamação não é a imputação da prática de algum crime pelo outro, mas a intenção difamatória de causar humilhação à pessoa ao expor fatos e suposições sobre sua vida privada.

Também existem os casos de bullying, com o advento da internet, a prática tomou uma proporção maior, já que o raio de aplicação se estendeu até o ponto em que através das redes sociais, a promoção de atividades que humilhem outrem pode ocorrer com uma frequência maior e ainda, sob a proteção do anonimato do agressor, que pode se esconder para praticar suas ações, que perpetuam na internet por um tempo indeterminável, já que, mesmo que a matéria da agressão seja excluída da rede, pode ter sido salva por inúmeros usuários desta.

A lei de combate ao bullying, 13.185/15, traz em seu teor a definição dos atos que configuram a conduta, que, segundo o próprio termo legal diz é uma forma de intimidação sistemática:

> Art. 1º Fica instituído o Programa de Combate à Intimidação Sistemática (Bullying) em todo o território nacional.§ 1º No contexto e para os fins desta Lei, considera-se intimidação sistemática (bullying) todo ato de violência física ou psicológica, intencional e repetitivo que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas (BRASIL, 2015).

A proteção à dignidade da pessoa humana, igualdade e liberdade está prevista na Constituição Federal, e busca amparar todo cidadão, evidenciando a responsabilização de todo aquele que ferir esses princípios. A discriminação racial é um crime caracterizado pela conduta preconceituosa e movida pelo ódio a pessoa de raça diferente, ocorrendo na maioria das vezes contra as pessoas negras.

Com o advento da internet, o crime de racismo encontrou um novo ambiente no qual as ações têm consequências até mesmo maiores que quando ocorrem num ambiente físico, já que a perpetuidade dos atos online acontece com grande frequência, aumentando muito o número de pessoas que são impactadas com as agressões racistas.

Compreende-se que a repercussão do crime de racismo nos meios digitais é muito grande, chegando a atingir um grande número de pessoas, já que o acesso aos dados inseridos na rede tem poucas limitações, quando as tem, levando os crimes cometidos nesse meio a

serem sujeitos a mesma consequência de quando a realização do ato criminoso é feita pessoalmente, e não usando uma ferramenta como a internet.

3. AUMENTO DO CRIME CIBERNÉTICO DURANTE A PANDEMIA DECORRENTE COVID-19

Recentemente, com o surgimento da pandemia do novo coronavírus (Covid19), uma das medidas mais adotadas ao redor do mundo foi o isolamento social, forçando a maioria das pessoas a adesão ao trabalho remoto visando diminuir ou evitar aglomerações nos espaços de trabalho e minimizar a proliferação do vírus. Com isso, acabou tendo um aumento gigantesco de aparelhos informáticos conectados simultaneamente, o que acabou por favorecer ainda mais a prática deste tipo de delito.

A sociedade de modo geral, além de ter que se preocupar com o Covid-19, crise política e econômica no país, a instabilidade financeira e emocional, causadas em parte pela pandemia, tiveram, também, que se atentar para a ocorrência dos crimes digitais. Com todo o caos gerado no país foi uma oportunidade para os criminosos e, por este motivo, os crimes digitais tiveram um crescimento alarmante. Segundo o relatório do Fortiguard Labs (Laboratório da Fortguard), no decorrer do ano de 2020 o brasil sofreu nada menos do que 8,5 bilhões de tentativas de ataques cibernéticos, sendo que, 5 bilhões ocorreram apenas nos últimos três meses do ano (outubro, novembro e dezembro).

No ano de 2021 o brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos, tendo um aumento de mais de 950% com relação a 2020 (com 8,5 bi), o brasil ocupou o segundo lugar em número de ataques na américa latina e caribe, atrás apenas do México (com 156 bi). A alta nos números foi constante durante o ano e ocorreu em toda a região, que chegou a registrar 289 bilhões de ataques no total, um crescimento de mais de 600% com relação ao ano anterior (com 41 bi).

Segundo os dados obtidos pelos Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos, apenas com relação as condutas abaixo: Maus Tratos Contra Animais, LGBTFobia; Neo Nazismo; Pornografia Infantil; Intolerância Religiosa; Xenofobia; Racismo; Violência ou Discriminação contra; Mulheres; Tráfico de Pessoas e Apologia e Incitação a crimes contra a Vida.

Em 2019, foram recebidas e processadas 75.671 denúncias anônimas envolvendo 39.864 páginas (URLs) distintas (das quais 24.319 foram removidas) escritas em 9 idiomas e hospedadas em 8.015 domínios diferentes, de 161 diferentes TLDs e conectados à Internet

através de 7.258 números IPs distintos, atribuídos para 65 países em 6 continentes. Em 2020, foram recebidas e processadas 156.692 denúncias anônimas de 74.011 páginas (URLs) distintas (43.316 delas foram removidas) escritas em 10 idiomas e hospedadas em 9.236 domínios diferentes, de 173 diferentes TLDs e conectados à Internet através de 8.524 números IPs distintos, atribuídos para 63 países em 6 continentes.

Em 2021, foram recebidas e processadas 150.095 denúncias anônimas envolvendo 71.095 páginas (URLs) distintas (das quais 32.538 foram removidas) escritas em 10 idiomas e hospedadas em 8.926 domínios diferentes, de 170 diferentes TLDs e conectados à Internet através de 9.900 números IPs distintos, atribuídos para 68 países em 6 continentes.

3.1 CRIMES DIGITAIS COMUNS NA PANDEMIA

O Malware, também conhecido como sequestro de dados, a distribuição de malware acontece por meio de publicidade enganosa, sites maliciosos e campanhas de phishing por e-mail foi a mais utilizada pelos cibercriminosos nos últimos anos, que no geral tentam roubar informações para ações maliciosas ou para a vender a outros criminosos para atividades futuras. Basicamente, é um vírus de resgate, que sequestra seus dados ou o controle de algum sistema. A partir disso, o criminoso começa a chantagear a vítima, exigindo um pagamento em troca dos dados. Uma vez que os dispositivos das vítimas forem infectados, podem ser controlados por invasores, que podem usá-los para cometer crimes, como roubo de credenciais, spam e ataques distribuídos de negação de serviço.

Já o Phishing ocorre quando o criminoso envia e-mail ou SMS (serviço de mensagens curtas) para a vítima, com links ou arquivos contaminados, que levam o usuário a um site. O objetivo do criminoso é enganar a vítima, fazendo com que ela forneça informações pessoais, como dados de conta bancária, por exemplo. O phishing é um dos crimes digitais mais elaborados, pois o golpista cria sites, aplicativos digitais e engana diversos usuários, de diferentes formas. Por exemplo, o criminoso cria sites falsos de compras online, com a mesma identidade visual e formato da loja original, o cliente passa a acreditar que está em um site confiável, realiza compras e fornece seus dados pessoais. Outro exemplo é a Clonagem do WhatsApp onde o criminoso encaminha um código de acesso ao aplicativo para o celular da vítima, entra em contato com a vítima se passando por alguma pessoa conhecida ou empresa. Com o código, o criminoso acessa o whatsapp da vítima, contendo todos os seus contatos e grupos de conversa no aplicativo. A partir disso, o golpista se passa pelo usuário e começa a mandar mensagens para amigos e familiares pedindo depósitos em dinheiro.

Crimes comuns também aumentaram durante a pandemia, a diferença é que agora elas acontecem no mundo digital; Calúnia a qual consiste em atribuir falsamente a alguém a autoria de um crime. Para que se configure o crime de calúnia, é preciso que seja narrado publicamente um fato criminoso. Um exemplo seria expor, na internet, o nome e foto de uma pessoa como autor de um homicídio, sem ter provas disso. Assim diz o artigo 138: "Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa".

A Difamação, que consiste em imputar a uma pessoa acontecimentos ofensivos à sua honra ou sua reputação, como por exemplo, espalhar mentiras, conversas infundadas, boatos que venham a afetar a reputação da pessoa no seu ambiente de trabalho ou meio social que está inserida. Seu artigo diz, "Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa".

O objetivo jurídico é a tutela da honra, e o respeito à personalidade do indivíduo. Ou seja, visa proteger a honra objetiva (reputação, boa fama, a maneira como é conhecido pela sociedade).

O crime de Injúria, que compreende em ofender a dignidade de alguém, como por exemplo, xingamentos, desacatos, palavras ofensivas e desrespeitosas, humilhações e etc. Vale lembrar que caso a ofensa seja relacionada a dignidade da pessoa, com elementos referentes a raça, etnia, religião, origem, pessoa idosa ou portadora de deficiência, a injúria será considerada como injúria qualificada. Seu artigo dispõe, "Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: -Pena - detenção, de um a seis meses, ou multa". Portanto, para que o crime aconteça de fato, é preciso que a injúria chegue ao conhecimento do ofendido ou de qualquer outra pessoa, pois se a ofensa proferida ou executada que não chegar ao conhecimento de ninguém, logo o crime não existirá juridicamente.

O crime de Ameaça que consiste em ameaçar outra pessoa, intimidando a pessoa com alguma coisa que pode lhe acontecer, por meio de palavras faladas ou escritas ou gestos, por exemplo, ameaçar alguém dizendo que vai matar algum familiar seu. Seu artigo diz: "Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave: Pena - detenção, de um a seis meses, ou multa. Parágrafo único - Somente se procede mediante representação".

Com este artigo a legislação quis protege a liberdade individual dos indivíduos, pois independentemente da realização ou não de um ato que fira a integridade física e ou moral de alguém, o simples fato de ameaçar em si, já se considera um crime.

O crime de Falsa identidade: mentir sua identidade ou a identidade de outra pessoa, com intuito de causar dano a alguém ou ganhar vantagem indevida. O artigo diz: Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave. Um exemplo claro deste delito é simples ato de criar um perfil "fake" nas redes, de uma pessoa real, estando ela viva ou morta, apenas isto já é suficiente para se enquadrar no delito descrito, pois implica que o criador do perfil falso se faz passar por outrem.

O estelionato: um dos crimes mais recorrentes do nosso ordenamento jurídico, o número de pessoas que tentam adquirir para si ou para outrem vantagem ilícita, aumenta tanto com ou sem o uso da internet. Seu artigo diz: Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. Resumindo é um crime onde o criminoso manipula, ilude e engana a vítima, induzindo-a a entregar bens e ou dados pessoais, voluntariamente, pois a vítima passa a acreditar equivocadamente que o estelionatário está agindo de boa-fé para com ela.

E o stalking: O crime consiste em uma forma de violência onde o sujeito infrator invade repetidamente a esfera da vida privada da vítima, por meio de atos que restringem a liberdade da vítima ou que ataquem diretamente a sua privacidade e ou reputação, resultando em um dano temporário ou mesmo permanente à integridade psicológica e emocional do indivíduo.

4. DO CONCEITO DE CRIMES CIBERNÉTICOS

Delitos virtuais são crimes que possuem uma peculiaridade, quer seja, são realizados contra ou através da tecnologia. Os autores também subdividem os delitos cibernéticos como: ações prejudiciais atípicas e crimes cibernéticos, sendo estes últimos divididos em crimes cibernéticos abertos e crimes cibernéticos exclusivos. (BRASIL, 2014)

Por definição, os crimes cibernéticos abertos são aqueles praticados por meio da tecnologia, sendo mero instrumento para a ocorrência do delito. Os crimes cibernéticos exclusivos, por sua vez, são os que ocorrem obrigatoriamente no meio virtual. No que concerne à lei brasileira, a tecnologia vem modificando a doutrina e jurisprudência e, de

forma que se entenda melhor os crimes da informática, a doutrina os divide em: próprios, impróprios, mistos ou complexos e mediatos ou indiretos. (BRASIL, 2014)

Os crimes impróprios são entendidos como aqueles em que a tecnologia está presente, mas não viola nenhum dos bens penalmente tutelado, de maneira, que para que seja enquadrado como crime, não é necessário ter conhecimento específico. (BRASIL, 2014)

Os crimes próprios, por sua vez, se enquadram nos casos em que o bem jurídico que se encontra sob tutela do direito penal é efetivamente violado. No caso dos crimes mistos ou complexos se entende que são delitos que somam mais de um tipo penal previsto, no caso em que, mais do que proteger os dados, se busque tutelar bem jurídico diverso. (BRASIL, 2014)

Para finalizar, os crimes mediatos ou indiretos são os casos em que o objetivo não é a informática, mas vem através desta, sendo o meio utilizado para que se permita a sua realização. (BRASIL, 2014)

A informática advém do uso de ferramentas para que consiga o tratamento automatizado da informação, sendo o copilado destas ferramentas o próprio computador.

O verbete *computador* como máquina feita de um núcleo variável unidades específicas regidas através de software que pode realizar diversas operações, sejam matemáticas, lógicas, administrativos e contábeis, sem que haja a interferência humana. (SILVA FELIPE, 2011)

Como sabido, *hardware* é a parte física dos computadores, quer seja, os componentes palpáveis, tais como, monitor, teclado, placas e afins. Os softwares por sua vez, são os programas que, através de sequências escritas em linguagem específica e que passam instruções para o *hardware*, permitindo que ele execute tarefas específicas. (SILVA FELIPE, 2011)

Computador, portanto, é união entre *hardware e software*. Um dos *softwares* mais utilizados para a realização de crimes são conhecidos como vírus, haja vista a rapidez de se proliferarem através da rede. Por definição os vírus são *softwares* com linhas de código leves que são acoplados ao um *link* ou outro arquivo, visando causar dano no computador de outrem. (SILVA FELIPE, 2011)

Os vírus mais comuns são “cavalos de troia” (*trojan horse*), *spywares* ou *keyloggers*, que são arquivos instalados no computador, disfarçado de programa útil, mas que, na realidade, acaba dando acesso para o criador do vírus à dados protegidos, como senhas, dados bancários e de cartões. (SILVA FELIPE, 2011)

Atualmente é sabido que pessoas com maiores conhecimentos de informática podem facilmente invadir e implantar vírus em quase qualquer computador, este tipo de pessoa é

rotulado de *hacker,* categoria emque se dividem entre "*hackers* éticos" e *crackers*. E são eles, portanto, os sujeitos ativos da maior parte dos crimes virtuais. (SILVA FELIPE, 2011)

Em meados de 1970, o mais conhecido dos criminosos cibernéticos era o indivíduo que possuía ao menos nível técnico em informática. Nos anos 80 os técnicos em informático receberam a companhia de empregados de empresas da área financeira como principais criminosos. (SILVA FELIPE, 2011)

No entanto, atualmente, qualquer pessoa pode praticar os crimes cibernéticos, tendo em conta as diversas oportunidades que as novas organizações e a própria tecnologia proporcionam. Alguns dos chamados *hackers* éticos inclusive, trabalham para o governo para solucionar problemas eventualmente causados por *crackers*. (SILVA FELIPE, 2011)

No exercício de suas funções é comum que os *hackers* invadam sistemas para corrigir eventuais falhas na segurança e instalar formas de defesa de forma que possam garantir a segurança dos acessos à informação daqueles computadores. Outrossim, ao invadir os sistemas os *hackers* éticos conseguem perceber as vulnerabilidades e contê-las para impedir que *crackers* os acessem. (SILVA FELIPE, 2011)

Os *hackers* não éticos, ou, também chamados *crackers*, como se presume, possuem finalidades destrutivas, através da invasão de servidores que facilitem o envio de informações maliciosas. (SILVA FELIPE, 2011)

Assim, se percebe que a área tecnológica contempla uma vasta gama de conceitos, o que a torna uma ciência bastante complexa.

No entanto, neste capítulo se logrou êxito em definir os conceitos mais importantes da informática, bem como a ligação entre informática e direito, ao se apresentar as conceituações jurídicas mais importantes neste contexto.

4.1 TIPOS DE CRIMES CIBERNÉTICOS

A Lei 12.737/2012 surgiu a partir do projeto de Lei nº 2.793/2011, que foi aprovado após o caso da atriz Carolina Dieckman, que teve seus dados acessados por crackers que, através de um e-mail infectado que atriz teria dado um click, acessaram seu computador pessoal, obtendo fotos íntimas da atriz, inclusive nua, e fotos familiares com o filho de apenas quatro anos de idade. Inicialmente cogitou-se a hipótese de a invasão ter sido feita na loja em que Carolina teria consertado o computador meses antes.

Logo depois, ficou comprovado que, de fato, foram hackers do interior de minas Gerais e de São Paulo que praticaram o delito. A atriz foi chantageada pelos criminosos que

exigiram o pagamento de R$ 10 mil para que as fotos não fossem divulgadas nas mídias sociais (MENDES, 2012).

Carolina registrou o boletim de ocorrência, quando foram iniciadas as investigações sobre o caso, três dias após a publicação das imagens a fim de evitar mais exposições. Como o Brasil não tinha uma lei específica para crimes de informática, os envolvidos foram indiciados por furto, extorsão qualificada e difamação, todos do Código Penal Brasileiro.

Antes do caso da atriz, muitas vítimas já eram registradas, no entanto, o caso ganh A Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709, de 14 de agosto de 2018) foi aprovada em 2018 e entraria em vigor a partir de 14 de agosto de 2020. Houve pedido de adiamento da vigência da lei para maio de 2021, mas a proposta foi rejeitada pelo Congresso, entrando a legislação em vigor em 18 de setembro. A lei representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil, tanto em meios físicos quanto em plataformas digitais. Além de mudar a maneira como instituições privadas coletam, armazenam e disponibilizam informações de usuários, a LGPD é destinada às instituições públicas – portanto, deve ser seguida por União, estados, Distrito Federal e municípios, ou destaque por se tratar de uma figura pública.

Embora o uso de computadores para cometer crimes não seja um fenômeno recente, a legislação brasileira ainda não está totalmente preparada para tipificar todas as formas de crimes cibernéticos. Atualmente, existe um projeto de lei e um Marco Brasileiro de Direitos na Internet para a Câmara dos Deputados e o Senado Federal, mas não há nenhuma disposição para que sejam considerados, votados e implementados. Tais documentos controlam, por exemplo, o crime de criação e transmissão de vírus e o pouco tempo que um provedor de internet deve manter registros de acesso de seus usuários. Esses aspectos jurídicos serão discutidos com mais detalhes no capítulo. Os principais recursos jurídicos estão disponíveis em Computer Forensic Expertise. Diante desse dilema, delegados e promotores têm utilizado a estratégia de criar atos ilícitos em casos existentes no Código Penal Brasileiro, evitando assim a punição dos infratores. É, portanto, muito importante distinguir se um computador é usado apenas como um auxílio para cometer crimes comuns ou se está sendo usado como um meio de cometer um crime. (QUEIROZ; IVARGAS, 2010).

4.2 O JUÍZO COMPETENTE

Nos crimes cibernéticos determinar o juízo competente é mais complexo haja vista que estes crimes são frequentemente cometidos contra qualquer um, independentemente do

local, e causam danos por vezes irreparáveis e de proporções incalculáveis. Desse modo, torna-se mister enfatizar a essencialidade da implementação de uma inteligência e uma expertise na inteligência da polícia para tornar mais eficaz as investigações, reduzindo a impunidade sobre esses crimes (SILVA; MARQUES, 2019).

É cediço esclarecer que para que esta política seja concretizada é preciso ter acesso às informações específicas acerca da incidência desses crimes e de suas condições, perfil das vítimas, o horário mais comum da prática criminosa e o *modus operandi* do crime, de uma política organizada que oriente e coordene setores responsáveis, primordialmente pela investigação dos crimes (SANTOS; MARTINS; TYBUCSH, 2017).

Elemento essencial na garantia da eficácia da ação do investigador é, ao ter ciência da prática de um crime cibernético, projetar qual foi o instrumento que os criminosos utilizaram para o ato ilícito. O crime pode ter se conformado com o uso de programas maliciosos, e-mails, websites, programas que propagam informações, grupos de debate, redes sociais, páginas de comércio eletrônico, entre inúmeros outros. De acordo com o meio utilizado para praticar o crime, distintas serão as ferramentas para se desvendar a autoria (CAVALCANTE, 2014).

Cavalcante (2014) defende que com a crescente utilização de smartphones, tablets e computadores portáteis, mais conexões sem fio ou redes wireless vão surgindo, o que permite acessar gratuitamente à internet. Contudo, estas conexões possibilitam o acesso de pessoas não identificadas, aumentando as oportunidades para criminosos, visto que dificultam sua localização, e facilitam a inserção com finalidade criminosa.

Nesse sentido, o combate ao crime cibernético também necessitou se moldar à nova realidade, posto que o progresso da tecnologia viabiliza o acesso absoluto dos criminosos ao mundo cibernético. Para conseguir a identidade de quem praticou ato ilícito na internet, é necessário solicitar aos provedores de aplicações de internet as informações de acesso do usuário que realizou determinada postagem (SILVA, 2017)

5. DOS CRIMES CIBERNÉTICOS EM ESPÉCIE

Atualmente, os crimes virtuais se tornaram bastante rotineiros e se proliferam, em sua maioria, através das redes socias, tais como Facebook e Twitter, que são as principais ferramentas para os crimes contra a honra, bastante comuns no meio virtual. (SILVA, 2007)

Nos dizeres de Fábio Moreira Freitas da Silva, no que tange aos crimes contra a honra:

Na internet, os crimes em especial de contra a honra, que podem ser calúnia, injúria e difamação, ocorrem com maior facilidade, pois a divulgação e a transmissão de informações na internet podem atingir a honra alheia, como qualquer outra mídia de uma forma muito rápida (SILVA, 2007).

Os crimes contra a honra são subdivididos em calúnia, injúria e difamação e tem suas ocorrências facilitadas na internet, tendo em conta que as notícias são transmitidas de forma facilitada através deste meio, maculando a honra alheia de maneira mais rápida e facilitada. (SILVA, 2007)

Como sabido, o Código Penal prevê três tipos de crime contra honra, quer sejam, calúnia, difamação e injúria, que se definem a seguir: (BRASIL, 2014)

A calúnia, conforme o art. 138 da legislação criminal, é se acusar a alguém, de modo falso, de conduta considerada criminosa. A difamação, por sua vez, de acordo com o previsto no artigo seguinte da mesma legislação, é imputar fato ofensivo a outrem. E, enfim, a injúria, estando positivada no artigo posterior da lei penal, é ofender a reputação de outra pessoa, independentemente da veracidade dos fatos. (BRASIL, 2014)

Quanto à qualificação destes delitos, Damásio E. de Jesus assevera que são crimes de perigo, tendo em conta que o agente não está intencionado à macular a reputação da vítima e expô-la à qualquer tipo de prejuízo, no entanto, da mesma forma, há o animus de se realizar a efetiva conduta jurídica tipificada. E, assim sendo, são delitos formalizados, cuja conceituação descreve a conduta do agente, bem como seu resultado, mas não exige que este seja efetivamente executado.

Desta forma, desnecessário, que o agente tenha êxito em sua empreitada, mas que suas condutas busquem desonrar a reputação do outro. (PIRES, 2016)

Defender o nome, a reputação, deve ser objetivo da sociedade, tendo em conta que é imperativo para a vida civilizada. (PIRES, 2016)

No mesmo espectro, há o bullying e este, como sabido, se define como ofensas repetidas focadas em uma determinada pessoa. Com a chegada da internet, nasceu o cyberbullying, que tem as mesmas ofensas do bullying, mas realizadas na internet. (PIRES, 2016)

Esta forma de abuso pode ocorrer de diversas maneiras e se disseminar rapidamente através das redes e que dificilmente podem ser exterminados da internet pela vítima. Ainda assim, são classificados como crimes contra a honra e podem ser classificados como tal. (PIRES, 2016)

Também deve-se mencionar crimes de preconceito por cor, etnia, religião, origem e condições sociais, que são nomeados de injúria racial ou racismo. Estes crimes também são praticados com frequência no meio digital. (PIRES, 2016)

Injúria racial, conforme prevista no art. 140, § 3 do Código Penal, é direcionada à uma determinada pessoa, tendo motivações referentes à raça, cor, etnia, condição social, idade ou se há deficiências. (PIRES, 2016)

O racismo, por sua vez, é no dano causado ao grupo que possui os mesmos elementos que se encontram arrolados no crime de injúria racial e está embasado na Lei 7716/1989, e visa segregar a sociedade. (PIRES, 2016)

Outra conduta bastante efetuada através das redes é a pedofilia, tendo a tecnologia atraído os pedófilos tendo em conta sua facilidade de se adquirir os conteúdos pornográficos (PIRES, 2016)

A tecnologia toca o indivíduo com maneiras únicas, permitindo-se formar comunidades online específicas para cada tipo de interesse, inclusive no caso da pedofilia. E, assim sendo, os pedófilos criaram suas próprias comunidades nas quais podem se comunicar uns com os outros, fortalecendo sua própria identidade. (PIRES, 2016)

Em seguida, a pedofilia é subdividida em aberta, conforme o previsto no art. 240 do ECA ou somente cibernética, prevista no art. 241-A da mesma legislação. (BRASIL, 2014)

Os doutrinadores também classificam os crimes de constrangimento ilegal (art. 146) e ameaça (art. 147) como praticados majoritariamente no meio virtual. (BRASIL, 2014)

Como exemplo, se pode citar o caso de Isadora Faber, uma estudante catarinense que criou uma página, que nomeou de “Diário de Classe”, que servia para expressar suas preocupações quanto à estrutura de sua escola. Logo a página ganhou sucesso e Isadora passou a sofrer ameaças, gerando comoção nacional diante do caso e ensejando denúncia do Ministério Público tendo em conta as ameaças. (SILVA, 2000)

Prosseguindo, espionagem é a modificação de softwares, através de mudanças na programação inicial de modo que se obtenha acesso à banco de dados ou registros e outras informações, sendo frequentemente acessadas diante de um local remoto através da rede. Assim sendo, o acesso sem razão e não autorizado de um sistema específico se configura como crime. Remy Gama Silva cita a espionagem no ambiente virtual lecionando acerca do tema da seguinte forma: (SILVA, 2000)

> A espionagem caracteriza-se pela alteração dos programas do computador que pode ser efetuado pela troca de cartões, discos ou fitas originais, por

> falsos, modificando-se assim a programação originária, promovendo o acesso ao banco de dados, registros, etc. O acesso intencional e injustificado de uma pessoa não autorizada pelo dono ou operador de um sistema de computador pode constituir um comportamento criminal. Este acesso é frequentemente realizado de um local remoto, ao longo de uma rede de telecomunicações, dentre outros meios (SILVA, 2000, p. 15).

Importa, nesse momento, que os e-mails, reconhecidos como cartas eletrônicas, são protegidos pela Constituição Federal de 1988 através de seu artigo 5º, XII. (BRASIL, 2014)

Interpretando de forma mais extensiva este dispositivo legal, Alcides Spoladore Filho assevera que mesmo que não se encontre positivado de maneira específica a inviolabilidade dos emails e outras mensagens como forma de comunicação através de nossa tecnologia pode ser assegurada pela proteção das correspondências, conforme o dispositivo constitucional citado supra. (SPOLADORE FILHO, 2011)

Por fim, se vê que o direito penal vem enfrentando diversos desafios no tocante aos novos tipos penais advindos da tecnologia ou de interpretar de forma extensiva as tipificadas anteriormente de forma que consiga proteger os bens jurídicos que estão sob sua guarda e se adaptar à rapidez dos avanços tecnológicos. (SPOLADORE FILHO, 2011)

Ademais, certos princípios constitucionais são importantes para servir de embasamento de forma a dirimir os conflitos atinentes à tecnologia. Pode-se se citar, nesta esteira, os princípios da dignidade da pessoa humana, livre manifestação do pensamento, bem como a livre expressão da atividade intelectual, artística, científica e de comunicação, de modo que seja realizada sem nenhum tipo de censura ou licença. Também se incluem o direito à honra, privacidade e imagem, o sigilo de correspondência e comunicação. (SPOLADORE FILHO, 2011)

6. PRINCÍPIOS CONSTITUCIONAIS ENVOLVIDOS

No que cabe à análise do relacionamento entre a tecnologia e o Direito Penal, cumpre perceber a importância que a Constituição Federal para o equilíbrio deste relacionamento, tendo em conta que a Carta Magna prevê princípios que regulam o convívio tênue entre os humanos e a tecnologias. (CARVALHO, 2005)

Muito embora o Direito Penal seja o balizador dos conflitos entre o indivíduo e o Estado, sendo que, por definição, o crime é a pior mácula que o indivíduo pode causar contra o Estado e a punição estatal a mais grave das formas de interferência na liberdade individual

e, assim sendo, a Constituição vem como reforço destes limites, de modo que se garanta a liberdade e a dignidade do indivíduo. (CARVALHO, 2005)

Kildare Gonçalves Carvalho faz as seguintes considerações:

> Sendo o Direito Penal instrumento de política social, erige-se em tema político por excelência, a partir do conflito entre o indivíduo e a autoridade estatal, considerando ainda que o crime constitui, em regra geral, o mais grave ataque que o indivíduo desfere contra bens sociais tutelados pelo Estado, e a sanção criminal a mais penetrante intervenção do Estado na esfera individual. As Constituições reforçam os limites constitucionais garantidores da liberdade, tanto no plano formal quanto no substancial, de modo a preservar a dignidade da pessoa humana. Assim, o Direito Penal é constitucionalmente valorizado, não só como limite à liberdade, mas como instrumento de liberdade individual. Chega-se até mesmo a falar, neste ponto, que o Direito Penal não apenas limita a liberdade, mas cria a liberdade (CARVALHO, 2005, p.19).

A intervenção constitucional, portanto, vem de forma a valorizar o Direito Penal, ao considera-lo importante instrumento tanto de criação quanto de manutenção das liberdades individuais. No entanto, resta claro que os tipos penais ainda não conseguem abraçar todas as possibilidades de lesão ao bem jurídico tutelado pelo Direito Penal, sendo, portanto, ineficientes em se tratando dos crimes cibernéticos. (CARVALHO, 2005)

Assim sendo, necessária uma conexão entre as relações humanas, a tecnologia e o meu jurídico. Na mesma medida em que a tecnologia e a globalização trouxeram inúmeros avanços, também acarretaram diversos problemas. (ANDRADE, 2008)

Se sabe que, atualmente, se consegue obter dados de forma rápida e dinâmica, tendo em conta o dinamismo da internet e da maneira com que a tecnologia agora faz parte da vida humana, de modo quase simbiótico. (ANDRADE, 2008). Nesse sentido vão os estudos de Allan Diego Mendes Melo de Andrade:

> Contudo, o desafio quanto a essa questão ainda revela-se instigante, uma vez que com o advento das novas tecnologias da informação, em especial a internet, o acesso e a divulgação de dados e informações ganharam uma dimensão pouco imaginável para os padrões tecnológicos de algumas décadas atrás. A interligação dos computadores através de uma rede mundial possibilitou grandes avanços no que se refere às comunicações e o surgimento de inúmeros serviços e recursos que antes estavam inseridos no dia-a-dia da humanidade (ANDRADE, 2008).

A doutrinadora Liliana Minardi Paesani também assevera que nunca, em nenhum período da história humana se conseguiu ter tanta informação copilada em um único local e com acesso tão dinâmico e rápido. Como exemplo, se pode citar o acesso a literaturas de todo o mundo, o recebimento de notícias em tempo quase real. (PAESANI, 2003)

> A informação está disponível. É possível acessar bibliotecas em todos os cantos do planeta. É possível receber a notícia no exato momento em que o fato acontece. É possível acompanhar as façanhas do ser humano, seus feitos prodigiosos ou suas catástrofes. Eis o milagre da informação em tempo real, como se diz. Em contrapartida, a vida privada da pessoa humana está cada vez mais desnudada por curiosos de toda natureza. Há interesses políticos, econômicos, sociais que tentam justificar tamanha invasão (PAESANI, 2003, p. 13).

No entanto, por óbvio que a privacidade ficou em segundo plano, em detrimento da facilidade com que correm as informações e esta invasão também se justifica por interesses políticos, sociais e econômicos. Em razão destes acontecimentos nascem costumes que exercem forte influência na forma de pensar dos Doutrinadores. (PAESANI, 2003)

Neste tocante, tem se o direito à informação, conforme previsto na Constituição Federal, bem como o direito a livre expressão da atividade intelectual, artística, científica, e outros, que se encontram em constante atrito com as modificações sociais dos últimos anos, tendo em conta o progresso da tecnologia. (PAESANI, 2003)

Estes direitos, da mesma forma, se chocam com outros que também possuem previsão constitucional, tais como intimidade, vida privada, honra e imagem, tendo em conta que com os avanços tecnológicos se facilita o rastreio da vida privada, de modo que se conhece detalhes íntimos e hábitos humanos, através das redes sociais ou de compras efetuadas com cartão e estas informações são retransmitidas facilmente. (PAESANI, 2003)

Se sabe que o mundo atual se encontra globalizado quase em sua totalidade e isto se deve aos avanços tecnológicos, que enseja uma homogeneização dos costumes e das culturas de consumo, de modo que os mesmos produtos são produzidos em escala global Em razão deste progresso, se quebraram as barreiras culturais, políticas e econômicas o que ensejou novos pensamentos doutrinários objetivando proteger interesses coletivos que possam ser quebrados em razão dos avanços da tecnologia. (PAESANI, 2003)

Nesta esteira, no momento em que a difusão dos dados de forma tão rápida que ocorre atualmente seria inimaginável há apenas algumas décadas atrás e foi possibilitada pela internet, que, como sabido, modificou por completo a forma com que os seres humanos se comunicam e o dinamismo com que passaram a pensar. (PAESANI, 2003)

Assim, nas palavras de Paesani:

> Sob o ponto de vista jurídico, ocorre o impasse do Direito ante o fato da globalização. Torna-se necessário estabelecer que o Direito é uma *ciência de segundo grau* e, como tal, depende do conhecimento da realidade a que se

> refere. Portanto, não basta conhecer a *norma*, é indispensável conhecer preliminarmente o *fenômeno* que se quer disciplinar por meio da lei, estudar as situações concretas em que será aplicada e prever s efeitos que surgirão da interação entre a situação de fato e o preceito normativo (PAESANI, 2003, p. 18).

Desta feita, é possível entender porque o Direito não possui meios de se integrar ao dinamismo da internet, tendo em conta o comportamento majoritariamente conservador que percebe no legislador. (PAESANI, 2003)

Assim sendo, se percebe a necessidade de uma mudança de pensamento por parte do legislador, de forma que ele consiga se adaptar às mudanças tecnológicas e, ao mesmo tempo, preservar os direitos do ser humano, em especial sua privacidade, de modo a se alcançar a justiça por qualquer eventual dano ocorrido. (PAESANI, 2003)

Desta forma se percebe que uma reforma constitucional brasileira é necessária para que esta se atualize e se evite qualquer injustiça e, também para que se acompanhe a rápida evolução social advinda das novas tecnologias, como demonstrado nas palavras de José Joaquim Gomes Canotilho:

> Os direitos fundamentais são estudados enquanto direitos jurídicos positivamente vigentes numa ordem constitucional. Como iremos ver, o local exato desta positivação jurídica é a constituição. A positivação dos direitos fundamentais significa a incorporação na ordem jurídica positiva dos direitos considerados "naturais" e "inalienáveis" do indivíduo. Não basta uma qualquer positivação. É necessário assinalar-lhes a dimensão de fundamental *rights* colocados no lugar do cimeiro das fontes de direito: as normas constitucionais. Sem esta positivação jurídica, os "direitos dos homens são esperanças, aspirações, ideias, impulsos, ou, até por vezes, mera retórica política", mas não direitos protegidos sob a forma de normas (regras e princípios) de direito constitucional (*Grundrechtsnormen*) (CANOTILHO, 1998, p. 347).

Ademais, se percebe que os direitos fundamentais são explorados sob a ótica que de são direitos constitucionais positivados, de maneira que seja possível agregá-los e considera-los como naturais e imutáveis. (CANOTILHO, 1998)

No entanto, o doutrinador assevera que mera positivação não é suficiente, é necessário que haja uma positivação sob o manto de direitos fundamentais, pois, sem esta positivação os direitos fundamentais são meras construções abstratas e não estão protegidos por lei. (CANOTILHO, 1998)

Desta forma, se percebe que o grande problema relacionado à regulamentação das tecnologias, mais especificamente à internet, é que esta não possui um local palpável em que

possa ser explorada, e a legislação atual enquadra apenas entidades mais tradicionais. (CANOTILHO, 1998)

Nesta esteira se percebe que o Direito, enquanto ciência secundária e, portanto, precisa se ater à realidade a que está adstrita, e, assim sendo, mero conhecimento da norma não é suficiente, é necessário, também, conhecer o contexto fático do que se busca proteger através do estudo das situações específicas em que tal regramento vai ser utilizado, de forma que se consiga antecipar os efeitos da norma e auferir se serão suficientes para regular aquela situação específica. (CANOTILHO, 1998)

Por estes ensinamentos é possível tecer uma conexão entre os princípios constitucionais e os crimes cibernéticos que os afronta. Tem-se que a dignidade da pessoa humana, prevista no art. 1º, inciso III, da Carta Magna é o basilar para a proteção das ações praticadas no meio virtual. Além destes, pode-se citar também a livre manifestação de pensamento, o direito à livre expressão da atividade intelectual, artística, científica e de comunicação aplicadas no ambiente virtual, que ensejam discussões no tocante aos limites impostos na relação entre liberdade de expressão e os bens que se encontram sob a tutela do Direito Penal. (CANOTILHO, 1998)

De fato, a proteção da honra e intimidade, também previstas na Constituição Federal, é o direito mais violado no meio virtual, bem como as violações de dados, sejam senhas ou e-mails. Por fim, a globalização trouxe, e vem trazendo, severas modificações na sociedade e, assim sendo, se percebe que a legislação não está preparada para proteger os direitos que possam ser violados em razão de tais mudanças, sendo este o grande desafio do Direito do século XXI, quer seja, se manter atualizado para proteger a sociedade no tocante ao dinamismo das redes, promovendo a responsabilização justa e adequada aos praticantes dos crimes cibernéticos. (CANOTILHO, 1998)

7. DOS CRIMES CIBERNÉTICOS NA INTERNET

Como nos traz o artigo 11 da Declaração dos Direitos do Homem e do Cidadão:

> Artigo 11º - A livre comunicação dos pensamentos e opiniões é um dos direitos mais preciosos do homem: todo cidadão pode, portanto, falar, escrever, imprimir livremente, embora deva responder pelo abuso dessa liberdade nos casos determinados pela lei.

Todos somos livres para fazer nossa escolha até que esse ato alcance a honra de outro e não o humilhe moralmente. E essa Lei nos garantiu esse dano.

Na verdade, várias são as dúvidas, uma delas é: "Até que ponto você pode expressar sua opinião no mundo virtual?"

A Internet deve ser vista como uma fonte ampla e liberal de muitas maneiras diferentes de pensar. Este é um espaço de debate de diferentes pontos de vista sobre o assunto, mas cada cidadão deve se responsabilizar por sua opinião. A pessoa tem direito à liberdade de expressão e opinião, também consagrada na Declaração Universal dos Direitos do Homem, cujo artigo XIX estabelece que:

“Toda pessoa tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de expressar livremente opiniões e de buscar, receber e transmitir informações e ideias por qualquer meio e independentemente de fronteiras. "

Isso é necessário para prevenir qualquer crime online. A liberdade de expressão é geralmente limitada. A pessoa tem o direito de expressar seus pensamentos, mas se falar de forma hostil ou lutar contra as Leis, a pessoa deve assumir o resultado de sua ação.

O comportamento digital é comum na prática do racismo, conforme estabelece a Lei 7.716 de 1989, cujo artigo 20 estabelece:

É crime induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou nacionalidade.

Nesse caso, a pena é de reclusão e multa de 2 (dois) a 3 (três) anos e multa. De fato, para os crimes contra a honra, quando o racismo é praticado na Internet, a pena pelo uso de redes sociais ou publicações de qualquer natureza pode ser aumentada de 2 (dois) para 5 (cinco) anos na prisão.

A partir do momento que você fala uma palavra, posta uma imagem ou vídeo na Internet, eles afetam outras pessoas, e os eventos que aconteceram não dependem de nossas intenções.

Os tribunais estão atualmente resolvendo vários casos de crimes online. No final das contas, porém, isso agrava a questão, pois tem consequências mais sérias.

Consequentemente, existem três tipos de crimes de honra que são abrangidos pelo Código Penal Brasileiro. A primeira previsão é calúnia, o que significa que uma pessoa cometeu um crime, o que não é realista;

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime.

Se a calúnia ocorrer através de um e-mail distribuído na internet, todas as pessoas que tiverem recebido o e-mail e passarem para frente podem ser envolvidas em coautoria. Pois diz que, a mesma pena incorre quem, sabendo que é falsa a imputação a propaga ou divulga. Os outros dois tipos são a difamação e a injúria.

> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação.
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro.

Quando houver uma ofensa, caso o ofensor se arrependa, caberá retratação pública.

Se tratando de injúria, nada mais é, qualquer ofensa à dignidade de alguém e difamação, é a imputação de ato ofensivo à reputação de alguém.

8. CONSIDERAÇÕES FINAIS

Os avanços tecnológicos são uma realidade que não deve ser deixada de lado, em especial pela legislação, tendo em conta que está permitindo enormes progressos para a humanidade, eis que é forma infindável de se obter informações, se comunicar e se divertir.

Portanto, não se pode que negar que no âmbito do Direito Penal ainda não é possível englobar de forma adequada todos os comportamentos que podem ser efetuados nas redes, tendo em conta esta tecnologia ser tão dinâmica.

Ademais, importa salientar quem o Código Penal, ainda em vigor, foi sancionado em 1940 e, naquela época, de tecnologia e sociedade mais simples, era mais claro o conceito de atitudes criminosas. Hoje, no entanto, diversas condutas criminosas são realizadas através das redes e estes comportamentos são variados e realizados em escalas diversas.

Ao se analisar o histórico, bem como os conceitos dos crimes cibernéticos, bem como suas espécies, pode se perceber que, no contexto jurídico, estas relações podem ser deveras complexas.

Mesmo que o histórico do advento da tecnologia remonte à época da Guerra Fria, a atual legislação brasileira ainda não está em condições de dissolver os conflitos provenientes da tecnologia.

Ademais, em razão das complicações atinentes à investigação dos crimes cibernéticos, seja pela dificuldade material em si, ou, tendo em conta que nem as autoridades nem a legislação se encontram preparadas para investigar este tipo específico de delito, aumenta a

sensação de que a rede é um local desprotegido, em que os criminosos são agraciados com o manto da impunidade, tornando este tipo de crime cada vez mais comum.

Em razão do exposto supra, também se percebe que muitos dos delitos provenientes da internet sequer são denunciados, sendo comum as atitudes passivas das vítimas, em razão da já citada sensação de impunidade no que concerne aos crimes cibernéticos.

Por fim, se percebe que os princípios que se encontram previstos na Carta Magna Brasileira podem, e devem ser aplicados por extensão e analogia aos crimes cibernéticos, por criarem bases fundamentais para a limitação do uso de informação proveniente da internet.

Desta forma, se nota que é necessário se ampliar o entendimento dos princípios da liberdade de expressão e de manifestação de pensamento; do direito à imagem, privacidade e à honra e o direito ao sigilo de correspondência.

No entanto, tendo em conta que nenhum dos direitos fundamentais é absoluto, sequer ilimitado, não se pode atingir um bem jurídico tutelado em detrimento de outro, sendo esta máxima levada em consideração quando do exercício destes direitos no meio virtual.

Pelo exposto, entende-se, por fim, que tanto os doutrinadores quanto os legisladores estão focados em criar formas efetivas de combater os crimes cibernéticos.

REFERÊNCIAS

ANDRADE, Allan Diego Mendes Melo de. **O direito à intimidade e à vida privada em face das novas tecnologias da informação.** Piauí, 2008. Artigo Científico.

ARAÚJO, Laíss Targino de; REIS, Sérgio Cabral de. **Responsabilidade Civil de provedores de conteúdo de internet.** Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10422&revista_caderno=17>. Acesso em: 05.set.2022

ATHENIENSE, Alexandre. **Perguntas e resposta sobre o Marco Civil da Internet.** Disponível em: <http://alexandre-atheniense.jusbrasil.com.br/noticias/2819686/perguntas-e-respostas-sobre-marco-civil-da-internet>. Acesso em: 05.set.2022

AURÉLIO. **Conceitos de computador e *internet*.** Disponível em: <http://www.dicionariodoaurelio.com/Computador.html> Acesso em: 05.set.2022

AZEVEDO, Camila Kuster de; ANDRADE, Bárbara Évelyn de Melo. **Crimes de calúnia, difamação, e invasão de privacidade em redes sociais.** Disponível em: <http://s.profissionaisti.com.br/wp-content/uploads/2011/11/Invas%C3%A3o-de-privacidade-em-redes-sociais.pdf>. Acesso em: 05.set.2022

BARRAL, Welber Oliveira. **Metodologia da Pesquisa Jurídica.** 4.ed. Belo Horizonte: Del Rey, 2010.

BITENCOURT, Cezar Roberto. **Código Penal Comentado.** 7ª ed. São Paulo: Saraiva, 2012.

BITENCOURT, Cezar Roberto. **Tratado de direito penal (parte especial).** 5. ed. São Paulo: Saraiva, 2006.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Planalto, 2014.

BRASIL. Decreto nº 678/92. **Pacto de São José da Costa Rica.** Brasília, DF: Planalto, 2014.

BRASIL. Decreto-Lei nº 2.848/40. **Código Penal Brasileiro.** Brasília: Planalto, 2014.

BRASIL. Lei nº 8.069/90. **Estatuto da Criança e do Adolescente.** Brasília, DF: Planalto, 2014.

BRASIL. Lei nº 12.737/12. **Lei sobre Tipificação Criminal de Delitos Informáticos.** Brasília, DF: Planalto, 2014.

BRASIL. Lei nº 12.965/14. **Marco Civil da *Internet*.** Brasília, DF: Planalto, 2014.

BRUNHARI, Andréa de Almeida; ZULIANI, Ênio Santarelli. **Princípios Constitucionais e Direito de Imagem.** Disponível em: <http://www.rkladvocacia.com/arquivos/artigos/art_srt_arquivo20130321174122.pdf> Acesso em: 12.set.2022

CABETTE, Eduardo Luiz Santos. **Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático.** Disponível em: <http://jus.com.br/artigos/23522/primeiras-impressoes-sobre-a-lei-n-12-737-12-e-o-crime-de-invasao-de-dispositivo-informatico>. Acesso em: 12.set.2022

CALDEIRA, Thiago Leite. **Crimes virtuais: insegurança no âmbito virtual.** Monografia – Faculdade de Direito Santos Agostinho – FADISA, Montes Claros, 2012.

CANOTILHO, José Joaquim Gomes. **Direito Constitucional.** 2. ed. Coimbra: Livraria Almedina, 1998.

CAPEZ, Fernando. **Código Penal Comentado.** 3ª ed. São Paulo: Saraiva, 2012.

CAPEZ, Fernando. **Curso de Direito Penal.** 12ª ed. São Paulo: Saraiva, 2012.

CARDOSO, Philipe Monteiro. **Entenda o que é o Marco Civil da Internet e quais mudanças trará para os usuários.** Disponível em: <http://jus.com.br/artigos/27240/entenda-o-que-e-o-marco-civil-da-internet-e-quais-mudancas-trara-para-os-usuarios>. Acesso em: 12.set.2022

CARRERA, Mário Sérgio Valadares. **A pedofilia virtual e seus reflexos no âmbito jurídico.** Disponível em: <http://www.viajus.com.br/viajus.php?pagina=artigos&id=803>. Acesso em: 12.set.2022

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17> Acesso em: 12.set.2022

CARVALHO, Kildare Gonçalves. **Direito Constitucional: Teoria do Estado e da Constituição Direito Constitucional Positivo.** 11ª ed. Belo Horizonte: Del Rey, 2005.

CARVALHO, Luiz Airton de. **Princípios Processuais Constitucionais**. Cartilha Jurídica – TRF 1ª região.1994. Disponível em: < www.TRF.jus.br>. Acesso em: 12.set.2022

COLARES, Rodrigo Guimarães. ***Cybercrimes*: os crimes na era da informática.** Disponível em: <http://egov.ufsc.br/portal/sites/default/files/anexos/5899-5891-1-PB.pdf>. Acesso em: 12.set.2022

COURI, Gustavo Fuscaldo. **Crimes pela internet.** Disponível em: <http://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/2semestre2009/trabalhos_22009/GustavoFuscaldoCouri.pdf>. Acesso em: 20/10/2022

DALL'AGNOLL, Isabel Costa Cabral. **Responsabilidade civil dos provedores de internet.** Disponível em: <http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2009_2/isabel_dallagnol.pdf>. Acesso em: 18.set.2022

DANTAS, Rosalliny Pinheiro. **A honra como objeto de proteção jurídica.** Disponível em:<www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11017revista_caderno=9>. Acesso em: 18.set.2022

DULLIUS, Aladio Anastacio; HIPLLER, Aldair; FRANCO, Elisa Lunardi. **Crimes praticados em ambientes virtuais.** Disponível em: <http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html> Acesso em: 18.set.2022

FARIAS, Cibelly. **O sigilo postal na era da comunicação digital.** Disponível em: <http://www.tresc.jus.br/site/resenhaeleitoral/edicoesimpressas/integra/arquivo/2012/junho/artigos/osigilopostalnaeradacomunicacaodigital/indexe79e.html?no_cache=1&cHash=5dd14ae47b9073d7076d4149f3cbe7c3> Acesso em: 18.set.2022

FELIPE, Everton Araújo da Silva. **Cibercrimes: um breve estudo sobre o mundo virtual e os crimes contra honra.** Disponível em: <http://repositorio.ucb.br/jspui/bitstream/10869/2162/1/Everton%20Araujo%20da%20Silva%20Felipe.pdf>. Acesso em: 18.set.2022

FERRAZ JÚNIOR, Tercio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado.** Disponível em: <http://www.terciosampaioferrazjr.com.br/?q=/publicacoes-cientificas/28> Acesso em: 18.set.2022

FERREIRA, Lóren Pinto. **Os "crimes de informática" no direito penal brasileiro.** Disponível em: <http://www.oab.org.br/editora/revista/revista_08/anexos/crimes_de_informatica.pdf>. Acesso em: 18.set.2022

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre ética informacional.** Disponível em: <http://www2.cjf.jus.br/ojs2/index.php/revcej/article/viewFile/523/704>. Acesso em: 20.set.2022

GATTO, Victor Henrique Gouveia. **Tipicidade penal dos crimes cometidos na *internet*.** Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9962&revista_caderno=17>. Acesso em: 20.set.2022

GUEDES, Igor Rafael de Matos Teixeira. **A pedofilia no âmbito da internet.** Monografia – Faculdades Integradas Pitágoras de Montes Claros, Montes Claros, 2009.

LAURÁDIO, Regiane Scoco. **Responsabilidade civil dos provedores de internet.** Disponível em: <http://www.anchieta.br/unianchieta/revistas/direito_new/pdf/direito15_7.pdf>. Acesso em: 20.set.2022

LELLIS, Leonardo Pessoa Moreira de. **Direito à imagem: uma garantia constitucional.** Disponível em: <http//http://solucaojuridica.wordpress.com/2011/04/12/direito-a-imagem/> Acesso em: 20.set.2022

LENZA, Pedro. **Direito Constitucional Esquematizado.** 16ª ed. São Paulo: Saraiva, 2012.

MARQUES, Andréa Gonzaga. **Direito à honra.** Disponível em: <http://www.tjdft.jus.br/institucional/imprensa/artigos/2010/direito-a-honra-andrea-neves-gonzaga-marques>. Acesso em: 20.set.2022

MATOS, Christiano Rocha de. **Uma análise da pedofilia a partir das publicações na rede mundial de computadores.** Disponível em: <http://jus.com.br/artigos/24595/uma-analise-da-pedofilia-a-partir-das-publicacoes-na-rede-mundial-de-computadores/2>. Acesso: 20.set.2022

MENDES, Geraldo César. **A violação nos crimes de honra na *internet* nos *sites* de relacionamento.** Disponível em: http//siaibib01.univali.br/pdf/Geraldo%20Mendes.pdf Acesso em: 20.set.2022

MORAES, Alexandre de. **Direito Constitucional**. 23.ed. São Paulo: Atlas, 2008.

MORAES, Paulo Francisco Cardoso. Publicação de artigo científico. **A vedação constitucional do anonimato aplicada à *internet*. O papel do Estado brasileiro na identificação dos usuários e responsabilidade dos provedores.** Disponível em <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9964&revista_caderno=17>. Acesso em: 10.out.2022

MORAIS, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à *internet*. O papel do Estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9964>. Acesso em: 10.out.2022

MORAL, Caio Fernando Yamamoto. **Crimes informáticos e sua perpetração contra honra praticados com o uso do computador.** Disponível em: <http://galileu.fundanet.br/revista/index.php/emtempo/article/viewArticle/271>. Acesso em: 10.out.2022

NIGRI, Tânia. **Sigilo de dados: os limites de sua inviolabilidade.** Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=1498>. Acesso em: 10.out.2022

NORONHA, E. Magalhães. **Direito Penal.** 33 ed. São Paulo: Saraiva, 1999.

PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil.** 2ª ed. São Paulo: Atlas, 2003.

PEREIRA, Wilson Medeiros. **Crime e Internet: Prevenção e Repressão.** Monografia – Universidade Estadual de Montes Claros – UNIMONTES, Montes Claros, 1999.

PIOLI, Roberta Raphaelli. **Lei Carolina Dieckmann traz inovações necessárias.** Disponível em: <http://www.conjur.com.br/2013-abr-07/roberta-pioli-lei-carolina-dieckmann-traz-inovacoes-necessarias>. Acesso em: 20.out.2022

PIRES, Hindenburgo F. **O surgimento dos primeiro computadores.** Disponível em: <http://www.educacaopublica.rj.gov.br/biblioteca/geografia/0016.html>. Acesso em: 20.out.2022

PRATES, Márcio de Souza. **A previsão dos crimes de informática na legislação penal brasileira.** Universidade Estadual de Montes Claros – UNIMONTES, Montes Claros, 2001.

RAMOS, Emerson Esmeraldo. **Furto de informação via internet.** Universidade Estadual de Montes Claros – UNIMONTES, Montes Claros, 2001.

REINALDO FILHO, Demócrito. **Julgados sobre a responsabilidade dos provedores.** Disponível em: <http://www.conjur.com.br/2011-fev-20/jurisprudencia-responsabilidade-provedores-internet>. Acesso em: 20.out.2022

REZENDE, Paulo A. D. **Sobre anonimato, privacidade e neutralidade com a internet.** Disponível em: < http://www.cic.unb.br/~rezende/trabs/anonimato.html>. Acesso em: 20.out.2022

ROVER, Tadeu. **Compartilhar ofensa em rede social gera dano moral.** Disponível em: <http://www.conjur.com.br/2013-dez-04/compartilhar-comentario-inveridico-ou-ofensivo-facebook-gera-dano-moral> Acesso em: 20.out.2022

RULLI NETO, Antônio; AZEVEDO, Renato A. **Novos paradigmas para a responsabilidade civil dos provedores de internet.** Disponível em: <http://por-leitores.jusbrasil.com.br/noticias/3161392/novos-paradigmas-para-a-responsabilidade-civil-de-provedores-na-internet>. Acesso em: 20.out.2022

SALES, Fábio Augusto Cornazzani; LIMA, Gisele Truzzi de; MIRANDA, Rodrigo Barros. **Privacidade e internet.** Disponível em: <http://www.truzzi.com.br/pdf/artigo-privacidade-internet-gisele-truzzi-fabio-augusto-cornazzani-sales-rodrigo-barros-de-miranda.pdf>. Acesso em: 20.out.2022

SANTOS, Sabrina Zamana dos. **A responsabilidade civil dos provedores de hospedagem e conteúdo de internet e a proteção dos direitos de personalidade.** Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11626&revista_caderno=17>. Acesso em: 20.out.2022

SILVA, Fábio Moreira Freitas da. **A necessidade de uma regulamentação jurídica para o mundo virtual.** Disponível em: <http://www.ic.ufmt.br:8080/c/document_library/get_file?p_l_id=58070&folderId=59705&name=DLFE-2180.pdf>. Acesso em: 20.out.2022

SILVA FELIPE, Everton Araújo da. **Cibercrimes: um breve estudo sobre o mundo virtual e os crimes contra a honra.** Trabalho de Conclusão de Curso. Pró-Reitoria de Graduação – Universidade Católica de Brasília, Brasília, 2011.

SILVA, Remy Gama. **Crimes de Informática.** 1ª ed. São Paulo: CopyMarket. com, 2000.

TEIXEIRA, Luisa Souto. **Pedofilia virtual e seus reflexos no âmbito jurídico.** Monografia – Faculdade de Direito Santos Agostinho, Montes Claros, 2012.