PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

CRIMES VIRTUAIS: UMA ANÁLISE DA FALTA DE TIPIFICAÇÃO LEGAL DOS CRIMES CIBERNÉTICOS

ORIENTANDO (A): BRUNO DE LUCCA RODRIGUES COSTA

ORIENTADOR (A): PROF. (A) EDWIGES CONCEIÇÃO CARVALHO CORRÊA

GOIÂNIA-GO
2021

BRUNO DE LUCCA RODRIGUES COSTA

CRIMES VIRTUAIS: UMA ANÁLISE DA FALTA DE TIPIFICAÇÃO LEGAL DOS CRIMES CIBERNÉTICOS

Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof. (a) Orientador (a): Edwiges Conceição Carvalho Corrêa

GOIÂNIA-GO
2021

BRUNO DE LUCCA RODRIGUES COSTA

CRIMES VIRTUAIS: UMA ANÁLISE DA FALTA DE TIPIFICAÇÃO LEGAL DOS CRIMES CIBERNÉTICOS

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador (a): Profa. Dra. Edwiges C. Carvalho Corrêa Nota

_____

Examinador (a) Convidado (a): Profa. Ms. Eufrosina Saraiva Silva Nota

RESUMO

Com as mudanças na sociedade contemporânea em virtude da globalização e dos avanços tecnológicos, a internet se tornou a maior rede de comunicação da atualidade, poderia até mesmo se afirmar que o uso da internet pode ser considerado atualmente um recurso básico para a população mundial, tal como é a água, a energia elétrica etc. A tal afirmação pode parecer absurda ou exagerada, mas se analisar o tema em questão, basicamente quase tudo é movido pelo uso da tecnologia e, consequentemente, pela rede mundial de computadores, a internet. Contudo, a internet tornou-se um novo caminho para a realização de delitos já praticados no mundo real, ampliando-se o número de ações relacionadas aos crimes na internet, em decorrência das várias formas de se praticar a violência no mundo virtual. Desta maneira, a facilidade do uso da internet traz consigo questões preocupantes acerca da utilização indevida, proporcionando também à coletividade, motivo pelo o qual o Direito Digital deve se adequar para prestar, de forma satisfativa à proteção dos cidadãos. Assim, o presente trabalho tem o objetivo de fazer uma análise acerca dos crimes virtuais, dos procedimentos investigativos e da legislação vigente em relação a esses delitos.

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

ABSTRACT

With the changes in contemporary society due to globalization and technological advances, the Internet has become the largest communication network today, it could even be affirmed that the use of the Internet can be considered currently a basic resource for the world population, such as water, electricity etc. This statement may seem absurd or exaggerated, but if you analyze the theme in question, basically almost everything is driven by the use of technology and, consequently, by the worldwide network of computers, the Internet. However, the Internet has become a new path for the realization of crimes already committed in the real world, increasing the number of actions related to crimes on the Internet, due to the various ways of practicing violence in the virtual world. Thus, the ease of use of the Internet brings with it worrying questions about misuse, also providing the collectivity, which is why digital law must adapt to provide, in a satisfactory way to the protection of citizens. Thus, the present work aims to make an analysis about virtual crimes, investigative procedures and current legislation in relation to these crimes.

Keywords: Internet. Cyber crimes. Digital law. Criminal law.

SUMÁRIO

INTRODUÇÃO

É válido supor que a sociedade tem passado por profundas transformações nas últimas décadas, há vários motivos e fatores que vem contribuindo para isso. Mas, o que mais tem influenciado no comportamento humano é a internet.

Hoje em dia, quase tudo é movido basicamente pelo uso das Tecnologias de Informação e Comunicação (TICs) e, consequentemente, pela rede mundial de computadores, a internet. Por ser a maior rede de comunicação da atualidade, torna-se essencial no cotidiano da sociedade, estudo, trabalho, lazer e até mesmo o comércio fazem o uso da internet para realizar as tarefas que lhe são propostas.

As relações sociais, foram beneficiadas pelo uso da internet, distâncias foram encurtadas através das redes sociais, tal ferramenta que permite o acesso a pessoas de qualquer faixa etária, possibilitando a comunicação através das trocas de mensagens, de fotos, de áudios e até mesmo chamadas de vídeos.

Na educação, a internet tem um grande papel, serve como auxílio, por disponibilizar o elevado volume de informações, permitindo que o conhecimento se prolifere de forma ágil e com extrema facilidade, apenas tendo acesso à internet. Até mesmo em tempos pandêmicos, a alternativa usada para que aulas e cursos dessem prosseguimento sem que sofressem alterações em seu calendário ou até mesmo o cancelamento do mesmo, foi a internet, que surgiu como um caminho possível para que houvesse o prosseguimento das atividades.

O comércio online vem crescendo bastante, lojas virtuais, serviços contratados através da rede, dão força para esse tipo de negócio bater de frente com o comércio tradicional, uns até ultrapassam estes. Verifica-se que, mesmo o comércio sendo tradicional, no caso trata-se daquele em que o consumidor vai diretamente ao estabelecimento físico do fornecedor, faz o uso da internet para divulgação de seus produtos e seus preços afim de chamar a clientela ou até mesmo conseguir novos clientes.

Desta forma, percebe-se que o mundo globalizado é marcado pelo surgimento de tecnologias que possibilitam a alta circulação de informações, pessoas e mercadorias. Todavia, com os grandes avanços surgem grandes responsabilidades, apesar desses benefícios e facilidades que a internet proporcionou às pessoas, há quem se utilize a internet para a prática de atividades delituosas, como as práticas de

crimes virtuais, podendo ser crimes já existentes no mundo real e cometido através da rede ou crimes próprios existentes que surgiram no mundo digital.

Diversos são os crimes a serem praticados através da internet, dentre os quais menciona-se a pedofilia, difamação, calúnia e injúrias (dos crimes contra a honra), que são crimes que podem ser cometidos no mundo real, e também, crimes que surgiram que precisam especificamente da tecnologia da informação para serem praticados, como são os casos de phishing, furtos por meio de home banking, furtos de dados, dentre inúmeros outros.

Se a vida coletiva se transformou radicalmente por influência da internet, os crimes também acompanharam essa mudança. Desta forma, trouxe consigo questões preocupantes acerca da utilização indevida de seus recursos, motivo pelo qual esses tipos de delitos vêm aumentando cada vez mais.

Durante a pandemia causada pelo novo coronavírus, os golpes financeiros cometidos através da internet cresceram assustadoramente. No período entre 20 de março e 18 de maio de 2020, a busca de informações pessoais e bancárias de brasileiros na chamada dark web cresceu 108%, segundo pesquisa feita pela Refinaria de Dados, empresa especializada na coleta e análise de informações digitais. O número de buscas diárias alcançou 19,2 milhões ante 9 milhões no período pré-covid. (EPOCA NEGÓCIOS, 2020).

Entretanto, a problemática do assunto é que a popularização da internet, em que pese a enorme facilidade que proporciona à coletividade, também traz consigo questões preocupantes acerca da utilização indevida, motivo pelo qual os procedimentos investigativos junto com a nossa legislação vigente do que se trata dos crimes virtuais se adeque para prestar de forma satisfativa à proteção estatal dos cidadãos.

Como dito anteriormente, os Crimes Virtuais sempre existiram, mas na pandemia houve um grande aumento desses delitos até por conta de muitas pessoas também estarem a todo momento conectados, e, na maioria das vezes muitas pessoas nem imaginam que podem ter seus dados acessados ou roubados por um simples “click” em um link que foi enviado por uma mensagem por exemplo. A falta de informação e de conhecimento a respeito do assunto por conta dos usuários dos dispositivos informáticos também facilita a vida desses criminosos, além das condutas

também não estarem muitas delas tipificadas, das penas serem brandas e outros motivos que acabam fomentando o aumento desses crimes.

Diante da complexidade do tema, o Direito precisa se adaptar à nova realidade para tutelar bens jurídicos e preservar a dignidade da pessoa humana, não só isso como também a ampliação de delegacias especializadas por todo território nacional e discorrer sobre os mecanismos de segurança capaz de inibir, identificar e coibir a ação e a propagação desses crimes.

Pretende-se com este trabalho, tendo o principal objetivo de analisar se a aplicação da legislação penal a respeito dos crimes virtuais está precisando ou não de melhorias. Além de, incitar a discussão e analisar o chamado crime virtual e a evolução no combate deste, fazendo algumas considerações a respeito do conceito, surgimento do Direito na internet, pena, ação penal, lei penal no espaço e lugar do crime, princípio da territorialidade e extraterritorialidade, por fim, a legislação vigente.

A metodologia a ser utilizada no presente trabalho será o método hipotético-dedutivo, utilizando o procedimento bibliográfico, realizado por meio de levantamento em material teórico e jurídico, além de outros recursos, como materiais que já versavam a respeito do assunto, sites de internet e livros.

1 EVOLUÇÃO DA INTERNET

Frutos de pesquisas da década de 1960, mais precisamente no ano de 1962 com intuito de contribuir na Guerra, a Força Aérea americana solicitou a um grupo de pesquisadores que começassem a trabalhar em um sistema de comunicação descentralizado, a fim de internalizar as comunicações importantes para o momento.

Em 1966 a DARPA (Defense Advanced Research Projects Agency), uma espécie de agencias de projetos voltados a pesquisas avançadas para defender o território norte-americano, iniciou testes e pesquisas com o objetivo de estabelecer conexão remota que permitisse a transmissão de dados entre dois locais, esse projeto foi batizado de ARPANET (Advanced Research Projects Agency Network), que em português significa Rede de Agências para Projetos de Pesquisas Avançadas, inicialmente a ideia era estabelecer a conexão de pontos de rede usando linhas telefônicas dedicadas. (LINK NACIONAL, 2021).

Mas apenas em 1969 foi possível fazer a primeira transmissão de dados entre a UCLA (Universidade da Califórnia em Los Angeles) e o Stanford Research Institute, que distavam cerca de 600 quilômetros. A primeira mensagem trocada foi a palavra “login”, mas por causa de uma queda de conexão, apenas as letras “lo” chegaram ao destino final. (LINK NACIONAL, 2021).

Entretanto, a internet em si, só passou a ser conhecida na década de 1980, cuja ideia central tinha como objetivo “uma espécie de associação mundial de computadores, todos interligados por meio de um conjunto de regras padronizadas que especificam o formato, a sincronização e a verificação de erro em comunicação de dados”, e esse conjunto de regras recebeu a denominação de protocolo. (MINISTÉRIO PÚBLICO FEDERAL, 2006).

Foi no ano de 1990 que a internet começou a alcançar a população em geral, em 1990 havia cerca de 2 milhões de pessoas conectadas à rede em todo o mundo, doze anos depois esse número passou para 604 milhões. Neste mesmo ano, o engenheiro inglês Tim Brernes-Lee criou a World Wide Web, permitindo a utilização de interface gráfica e a invenção de site dinâmicos, permitindo que o usuário possa percorrer as páginas na rede (isto é, “navegar”), a partir de sequências associativas (links). (MINISTÉRIO PÚBLICO FEDERAL, 2006).

A internet foi criada para ser utilizada inicialmente para os vieses militares, culturais e acadêmicos. O seu crescimento foi muito rápido, e para facilitar o acesso dos usuários, surgiram navegadores (browsers) como a Internet Explorer da Microsoft. Assim, passou a ser utilizada por diversos segmentos sociais, como compras, vendas e entretenimento. Em 2006, começou uma nova era da internet com o avanço de redes sociais e a interação entre as pessoas no mundo virtual foi se tornando comum.

1.1 Internet e o Brasil

A primeira conexão entre Brasil e a internet, aconteceu no Rio de Janeiro, quando o Laboratório Nacional de Computação Científica (LNCC), conseguiu em 1988, uma conexão brasileira com a Universidade de Maryland, nos Estados Unidos. Onde a comunicação se restringia a e-mails e compartilhamento de arquivos, de forma individual e por linha telefônica. Um ano depois, em 1989, foi criada a RNP (Rede nacional de Pesquisa), que contou com apoio do CNPq (Conselho de Pesquisa Científica) e do governo José Sarney. (LINK NACIONAL, 2021).

De lá para cá, houve pouco investimento no setor e somente com a emblemática Eco-92 ou Rio 92, é que se pode dizer que decorreu o primeiro evento com “net” no Brasil, o que efetivamente fez a internet acontecer foi o comprometimento da ONU em estruturar o evento, numa força-tarefa, cedendo o provedor Alternex e RNP. (LINK NACIONAL, 2021).

Hoje em dia, o Brasil é um dos países que mais tem usuários conectados à internet, ficando atrás apenas da China, da Índia e dos Estados Unidos da América, isso com base na pesquisa feita pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD, na sigla em inglês). De acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE) os celulares foram os grandes responsáveis pela expansão do acesso à internet nos domicílios brasileiros. Pela pesquisa, o celular foi o equipamento utilizado por 94,6% das pessoas que acessaram a rede em 2016. O acesso móvel está acima de 90% em todas as grandes regiões. Apesar de o celular ser predominante, outras formas de acesso à rede são via microcomputador (63,7%), tablet (16,4%) e televisão (11,3%). (IBGE, 2018).

Um grande acontecimento no Brasil em relação a internet foi em 2014, quando a então Presidente Dilma Rousseff, sancionou a Lei 12.965, chamada de Marco Civil

da Internet, lei essa que regula o uso da internet no Brasil. Após surgir muitos casos de crimes praticados virtualmente e com o intuito de determinar direitos e deveres aos cidadãos/usuários da internet, essa lei surgiu com a pretensão de ser a constituição da internet no país.

2 CRIMES VIRTUAIS

Ressalta a necessidade de discutir a terminologia empregada pela comunidade jurídica em geral, há quem defina como cybercrimes, crimes informáticos, crimes virtuais, delitos digitais. É natural a variedade de definições, tendo em vista que esse novo campo de estudo e aplicação do direito se quer tem legislação robusta para tratar do tema, estamos acompanhando as primeiras considerações acerca da matéria. Entretanto, parece mais acertado o uso de crimes virtuais, por compreender todos os delitos praticados no meio virtual ou que se utiliza da web como favorecimento a pratica delitiva.

2.1 Conceito de Crimes Virtuais

Diante da problemática de se conceituar o que é crime virtual, dispõe ROSSINI:

> o conceito de 'delito informático' poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade. (2004, p. 110)

Importante salientar o conceito de "crime de informática", delineado pela Organização para Cooperação Econômica e Desenvolvimento da ONU: "O crime de informática é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento de dados e/ou transmissão de dados" (ROSSINI, 2004, p.109). Assim como dito acima, existem várias denominações se tratando de crime virtual, em alguns nem a necessidade de conexão à internet precisa, já em outros a conexão com a internet serve como intermediário para que o crime aconteça.

Por outro lado, CASTRO (2003, p. 09), levando em consideração o contido na Convenção sobre o Cibercrime de Budapeste em 2001, aduz que "os crimes de informática são aqueles perpetrados através dos computadores, contra os mesmos, ou através dele. A maioria dos crimes são praticados através da internet, e o meio usualmente utilizado é o computador."

Já a Lei dos Crimes Cibernéticos (12.737/2012), conhecida como Lei Carolina Dieckmann, faz a tipificação de atos como invadir computadores, violar dados de usuários ou “derrubar” sites.

Na concepção de FELICIANO, apresenta um conceito amplo de crime cibernético, por ele definido como crimes informáticos:

> Conheço por criminalidade informática o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware, software, redes, etc.). (2000, p.42)

A doutrina ainda se ocupa de distinguir os crimes cibernéticos em dois, crimes puros ou próprios e os impróprios, o caráter determinante para estabelecer a diferença, em suma é que nos crimes próprios, eles são cometidos somente na web, enquanto que aqueles, impróprios, o agente se utiliza da rede para ter facilitada sua conduta delitiva.

2.2 Tipos de Crimes Virtuais

Assim como existem diversas denominações, os crimes que são praticados no ambiente virtual também são variados.

Inclusive, alguns dos crimes que são praticados por meio da internet, já tem previsão legal na nossa lei penal, mas não necessariamente são tratados como crimes virtuais e sim como crimes penais, como por exemplo:

Quadro 1 – TIPOS DE CRIMES VIRTUAIS	
Calúnia – art. 138 do Código Penal (C.P.)	Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena – detenção, de seis meses a dois anos, e multa.
Difamação – art. 139 do C.P.	Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena – detenção, de três meses a um ano, e multa.
Injúria – art. 140 do C.P.	Injuria alguém, ofendendo-lhe a dignidade ou o decoro: Pena – detenção, de um a seis meses, ou multa.

Ameaça – art. 147 do C.P.	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.
Dano – art. 163 do C.P.	Crime de dano – destruir, inutilizar ou deteriorar coisa alheia: Pena – detenção, de um a seis meses, ou multa.
Apropriação indébita – art. 168 do C.P.	Apropriar-se de coisa alheia móvel, de que tem a posse ou a detenção: Pena – reclusão, de um a quatro anos, e multa.
Estelionato – art. 171 do C.P.	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.
Violação ao Direito Autoral – art. 184 do C.P.	Violar direitos de autor e os que lhe são conexos: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.
Pedofilia – art. 247 da Lei 8.069/90 Estatuto da Criança e do Adolescente	Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena – reclusão, de dois a quatro anos, e multa.
Interceptação de Comunicações de Informática – art. 10 da Lei 9.296/96	Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena – reclusão, de dois a quatro anos, e multa.
Interceptação de E-mail comercial ou pessoal – art. 10 da Lei 9.296/96	Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena – reclusão, de dois a quatro anos, e multa.

Crimes contra Software – "Pirataria" – art. 12 da Lei 9.609/98	Violar direitos de autor de programa de computador: Pena – detenção de seis meses a dois anos ou multa.
Phishing	Usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais.
Vírus cavalo de troia	É um tipo de malware que, frequentemente, está disfarçado de software legítimo. São utilizados para obter acesso aos sistemas dos usuários. Uma vez ativados, os cavalos de troia permitem que os criminosos o espionem, roubem seus dados confidenciais e obtenham acesso ao seu sistema pela porta de fundo.
Ransomware	É um tipo de software malicioso (malware) utilizado por cibercriminosos para infectar um computador ou uma rede, bloqueando o acesso ao sistema e criptografando os dados. Acontece muito quando os criminosos invadem sistemas de lojas ou mercados e pegam os dados de clientes para uma possível negociação de resgate em dinheiro.

Fonte: Código Penal Brasileiro (2020 Atualizado) e Canal Tech: O que é vírus, cavalo de troia etc.

Adaptado por BRUNO DE LUCCA, 2021.

No Quadro 1, está presente vários tipos de crimes que são possíveis de acontecer no âmbito real e virtual, tanto que a maioria deles listados são tipificados no nosso Código Penal, alguns exemplos citados são delitos cometidos somente possível de serem consumados pelo ambiente virtual, esses não são tipificados, portanto merecem uma importância maior e devem ser tratados com seriedade para que sejam tipificados no nosso código e que assim não fomentem a prática de tais delitos.

2.3 Classificação dos Crimes Virtuais

Como a característica dos crimes cibernéticos, assim como a internet, são muito dinâmicos, as classificações dos crimes cibernéticos devem sempre estar se ajustando às mudanças que tal prática delitiva apresenta no mundo virtual. FERREIRA faz sugestão para a classificação ao tema em questão, vejamos:

> Atos dirigidos contra um sistema de informática, tendo como subespécies, atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial. (2005, p.261)

Outras duas classificações, que são as mais usadas nos dias de hoje, também despontam na doutrina. A primeira classifica os crimes cibernéticos em puros, mistos e comum, enquanto a segunda divide os crimes de informática em próprios e impróprios.

Os crimes cibernéticos puros, segundo COSTA (1997, p.03) seriam “toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.”

Por outro lado, os crimes cibernéticos mistos, na lição trazida por PINHEIRO (2000, n.p.), “são aqueles em que o uso da internet ou sistema informático é condição sine qua non para a efetivação da conduta, embora o bem jurídico visado seja diverso ao informático.”

Por fim, os crimes cibernéticos comuns seriam aqueles em que a finalidade do agente é utilizar da internet ou sistema de informática para atingir um bem já tutelado. Nesse caso, a informática é um mero instrumento, não sendo indispensável para que o crime seja consumado.

2.4 Crimes Cibernéticos Próprios

Os crimes cibernéticos próprios, o agente visa atingir especificamente o sistema de informática ou os dados armazenados nos referidos sistemas, tais como as condutas praticadas por crackers, pessoas que utilizam de seu vasto conhecimento informático para invadir sistema com a intenção de causar danos aos sistemas informatizados. Então, de uma forma resumida, os crimes cibernéticos comuns seriam aqueles em que o objetivo do agente é de utilizar da internet ou sistema de informática para atingir um bem já tutelado penal. Ou seja, a informática é mero instrumento, não indispensável, para a pratica delitiva.

2.5 Crimes Cibernéticos Impróprios

Ao contrário do são os crimes cibernéticos próprios, os impróprios, seriam aqueles em que a utilização do sistema de informática trata-se apenas de um novo modus operandi, ou seja, um novo meio de execução, como o qual o agente visa atingir um bem já tutelado penalmente, diverso do sistema de dados ou informação. São exemplos os crimes contra o patrimônio, como o furto e o estelionato praticados com o uso da internet.

2.6 Hacker e Cracker

Inicialmente, o hacker não era visto sendo sinônimo de coisa boa, por ter um amplo conhecimento sobre a informática, sistemas entre outros. Apesar de serem palavras parecidas, hacker e cracker possuem significados diferentes. Os hackers são indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas. O nosso sistema eleitoral inclusive, conta com a ajuda de hackers para que não ocorra nenhum tipo de fraude nas eleições, os sistemas são analisados e cuidado por eles. Já os crackers são pessoas que praticam a quebra de um sistema de segurança. (CANAL TECH, 2019).

Os dois termos podem ser vistos como o lado bom e o lado ruim da força tecnológica, enquanto um utiliza seu conhecimento para melhorar softwares de forma legal e não invadir um sistema com intuito de causar danos, o outro utiliza e têm como prática a quebra de segurança e usam o seu conhecimento de forma ilegal, se tornando assim, criminosos.

As denominações foram criadas para que, as pessoas e, especialmente a mídia, não confundissem os dois grupos.

2.7 Deep Web

Deep Web (Internet Profunda, em tradução livre) é uma área da Internet que fica “escondida” e tem pouca regulamentação. O termo ficou mais conhecido no Brasil

depois do massacre de Suzano, em que dois jovens invadiram uma escola, mataram oito pessoas e depois se suicidaram. (TECH TUDO, 2019).

A Deep Web não pode ser acessada por meio de pesquisas em buscadores, como o Google ou Bing e também não é acessada digitando um endereço em um navegador comum (Chrome, Firefox, Edge etc). Justamente pela dificuldade de acesso, é usada para o compartilhamento de conteúdo ilegal, como venda de drogas, pedofilia e violência. (TECH TUDO, 2019).

Neste sentido, diversos pesquisadores apontam que a parte desconhecida pelo maior número de usuários da internet convencional, compreende 90% de toda rede. Ou seja, nela pode se encontrar de tudo. No que diz respeito ao tamanho desse universo virtual, Michael Bergman afirma que:

> [...] informações públicas na Deep Web são comumente de 400 a 500 vezes maiores que as definidas da World Wide Web. A Deep Web contém 7.500 terabytes de informações comparadas a 19 terabytes de informação da Surface Web. A Deep Web contém aproximadamente 550 bilhões de documentos individuais comparados com 1 bilhão da Surface Web. Existem mais de duzentos mil sites atualmente na Deep Web. Seis das maiores enciclopédias da Deep Web contém cerca de 750 terabytes de informação, suficiente para exceder o tamanho da Surface Web quatro vezes. Em média, os sites da Deep Web recebem 50% mais tráfego mensal, ainda que não sejam conhecidos pelo público em geral. A Deep Web é a categoria que mais cresce no número de novas informações sobre a Internet. Deep Web tende a ser mais estrita, com conteúdo mais profundo, do que sites convencionais. A profundidade de conteúdo de qualidade total da Deep Web é de 1.000 a 2.000 mil vezes maior que a da superfície. O conteúdo da Deep Web é altamente relevante para todas as necessidades de informação, mercado e domínio. Mais da metade do conteúdo da Deep Web reside em tópicos específicos em bancos de dados. Um total 95% da Deep Web é informação acessível ao público não sujeita a taxas ou assinaturas [...] (2013, p.441)

Vale dizer que a deep web é dividida em camadas, sendo que quanto mais profunda é proporcionalmente obscura e de difícil acesso. O principal apelo da deep web é a segurança e preservação do anonimato, visto que as informações não são rastreadas diretamente. Ao contrário, o sistema sigiloso, para garantir o anonimato e segurança dos usuários, só permite o acesso às demais camadas quando fornecida uma combinação de letras criptografadas, e muitas vezes de acesso restrito, de forma que a navegação seja distribuída por diversos caminhos, não sendo possível ir direto à fonte das informações que estão sendo trocadas. (FERNANDO JI HOON YU, 2020).

Acessar a deep web não é ilegal, inclusive ela é usada por empresas como forma de compartilhar informações com segurança. Ocorre que, o que se busca discutir, porém, é o amplo acesso da população à Internet, em contraponto, à falta de

conscientização da importância da prevenção, o que reflete outra fragilidade da Internet.

Apesar de existir há muito tempo, a internet dark vem ganhando, repercussão internacional. Visto que, com o aumento de sua utilização, atrelado ao crescimento significativo do acesso da população mundial à internet, facilitou pratica de crimes como pedofilia, tráfico de armas, de drogas, de órgãos, roubo de dados e ação de hackers que conseguem invadir, programas sigilosos de empresas e órgãos públicos, com intuito de furtar dados e compartilhar informações sigilosas

3 DIREITO E A INTERNET

Diz a locução romana: *Ubi homo, ibi societas. Ubi societas, ibi ius. Ergo ubi homo, ibi ius* – Onde há homem, há sociedade. Onde há sociedade, há Direito. Alguns doutrinadores fazem o seguinte arranjo, para a locução criminológica, num sentido mais crítico e reflexivo: *Ubi homo, ibi societas. Ubi societas, ibi crimen. Ergo ubi homo, ibi crimen* – Onde há homem, há sociedade. Onde há sociedade, há crime. Consequentemente, onde há homem, há crime. (DICIO, 2021).

E no meio virtual não é diferente, há milhares de pessoas conectadas, seja por diferentes motivos ou não, o ser humano já não consegue mais conviver sem a informática e a internet; esse mundo já faz parte de suas atividades diárias, tanto no campo profissional como na própria vida familiar e no lazer.

Por conta disso, o Direito encontra-se diante de um grande desafio, algo totalmente distinto daquelas relações que se buscava regular há sessenta anos. A nova era da sociedade digital, precisa que o Direito acompanhe essa nova realidade, que estabeleça a regulação pertinente, antes que a informática e a internet se transformem em feras indomáveis.

Isso deve acontecer pois os noticiários dos jornais, praticamente todas as semanas, trazem informações acerca de crimes cometidos no âmbito virtual, lesando milhares de pessoas. Até em meios que não se espera que aconteça isso, acabam acontecendo, como foi no caso da invasão de crackers no site do TSE (Tribunal Superior Eleitoral), onde a ação modificou temporariamente a página da internet, ato que levantou dúvida acerca da segurança do voto eletrônico, um assunto que foi levantado até pelo Presidente da República do Brasil.

Além disso, a influência da informática ocorre em vários ramos do Direito, por exemplo, os contratos eletrônicos, nas relações de compra e venda do ramo do Direito Civil e do Direito do Consumidor. No Direito Penal e Processual Penal, também houve mudanças, com a criações de leis especificas sobres crimes cibernéticos.

Nesse sentido, alude REALE:

> O direito é, por conseguinte, um fato ou fenômeno social; não existe senão na sociedade e não pode ser concebido fora dela. Uma das características da realidade jurídica é, como se vê, a sua socialidade, a sua qualidade de ser social. (2002, p.2)

O Direito Digital surge com o estabelecimento da internet e todas as suas situações sociais, políticas, econômicas e jurídicas. A jurista PINHEIRO aponta algumas situações que são tratadas pelo Direito Digital:

> A possibilidade de visibilidade do mundo atual traz também riscos inerentes à acessibilidade, tais como segurança da informação, concorrência desleal, plágio, sabotagem por hacker, entre outros. Assim na mesma velocidade da evolução da rede, em virtude do relativo anonimato proporcionado pela internet, crescem os crimes, as reclamações devido a infrações ao Código de Defesa do Consumidor, as infrações à propriedade intelectual, marcas e patentes, entre outras. (2009, p.76)

Nesse sentido, a ausência de normas especificas para as situações no âmbito da internet é um fator que fomenta a impunidade, pois devido às peculiaridades dos ilícitos, várias condutas continuam sem tipicidade, e assim, sem penalização.

Sobre o tema, cuida destacar as palavras do Ministro Raul Araújo, do Superior Tribunal de Justiça (STJ) rebatendo as críticas acerca da regulamentação da web, transcrevida através do site do CONJUR:

> A internet não é um universo sem lei. Os julgados do STJ retratam o cenário atual no Brasil ao mostrar que a internet é um espaço de liberdade, muito valioso para a busca de informações e o contato entre as pessoas, mas também de responsabilidade", explica o ministro Raul Araújo. "O Judiciário está atento ao direito das pessoas que têm a sua imagem violada. E os agressores, que imaginam estar encobertos pelo anonimato, serão devidamente responsabilizados por suas condutas. (2015, n.p.)

Em relação à regulamentação, cada país adota uma legislação própria, no que toca a Deep Web, foi criado um tratado internacional conhecido como Convenção de Budapeste a fim de discutir e regulamentar parâmetros para o cibercrime a nível mundial. (FERNANDO JI HOON YU, 2020).

Assevera CHAWKI sobre o assunto:

> [...] persiste a necessidade de estabelecer normas globais e padrões para reger a conduta e comportamento no mundo virtual. Apesar da necessidade, as políticas nacionais e regionais podem colidir com essa normatização global. Isto exige regulamentação universal ou global considerando o impacto transnacional e arrebatador inerente do cybercrime. Apesar da dificuldade intrínseca na harmonização ou unificação de políticas criminais e penais, sendo uma manifestação de poder soberano e autoridade, as participações no ciberespaço têm instigado os Estados a trilharem por uma nova época de cooperação em matéria de direito penal e público território irregular e vacilante. [...] O objetivo principal da Convenção é harmonizar a legislação penal material e procedimentos de investigação internas. Eram duas as principais preocupações dos redatores da Convenção: a primeira era assegurar que as definições fossem flexíveis a ponto de se amoldar aos novos tipos de crimes e seus métodos e a segunda era manter-se sensível aos regimes jurídicos dos Estados-nação. Estas preocupações foram

> especialmente desafiadoras na área de direitos humanos, porque os estados têm diferentes valores morais e culturais. Por exemplo, os países europeus têm um grau muito mais elevado de proteção da privacidade do que os Estados Unidos (2006, n.p.)

No entanto, deve-se dizer que o combate é ineficaz, uma vez que, a atual regulamentação, no que diz respeito às formas de punir os crimes, não consegue atingir seu objetivo pois o cyber-criminoso escapa facilmente do alcance da lei, já que consegue transpor as fronteiras de seus país e o seu reconhecimento ser impossibilitado devido ao anonimato garantido pela Deep Web. Nesse sentido alude SILVA:

> [...] Partindo de uma análise perfunctória da relação estabelecida entre o meio eletrônico com o homem, é possível a previsibilidade de chances maiores no cometimento de delitos no cyber espaço, tendo em vista que o usuário de tal meio se sente inatingível pela punição decorrente de um delito praticado por meio eletrônico, face à insegurança jurídica e a falta de preparação por parte do Estado, em dar continuidade às investigações, ou até mesmo de como proceder à investigação de delitos desta classe. Percebe-se de forma indutiva que muitos indivíduos que não seriam capazes de cometer delitos nas relações concretas (indivíduo x indivíduo), encontram no meio virtual segurança para o cometimento de delitos, seja tendo o virtual como meio (tráfico de drogas), seja como forma direta de prática de crime (estelionato) [...]. (2015, n.p.)

No Brasil a preocupação em regulamentar o uso da internet, inclusive a deep web, é fato novo, especialmente nas últimas décadas, isso porque, o aumento do acesso à tecnologia acabou por inserir na Constituição Federal de 1988, disposições relativas às leis de competência do Estado sobre questões de informática.

Ademais, a Lei nº 12.737/2012, conhecida como a “Lei dos Crimes Cibernéticos”, conhecida também como Lei Carolina Dieckmann, tem se revelado insuficiente para repreender os crimes dessa natureza, por não tipificar todas as condutas possíveis no universo da Deep Web.

4 JURISDIÇÃO, COMPETÊNCIA E LEGISLAÇÃO

A responsabilidade do Estado, através de seu papel regulador e fiscalizador, é de suma importância para que encontre formas de prevenção e combate às ilicitudes realizadas no âmbito virtual. E são por meio das jurisdições, das competências e nossas legislações que consiste na evolução do próprio Direito e também se tratando do futuro do Direito Digital que vem crescendo ao passar dos anos.

4.1 Jurisdição

Jurisdição é o poder que o Estado detém para aplicar o direito a um determinado caso, com o objetivo de solucionar conflitos de interesses e com isso resguardar a ordem jurídica e a autoridade da lei.

No sentido coloquial, jurisdição é a área territorial (município, estado, região ou país) sobre o qual este poder é exercido por determinada autoridade ou Juízo.

A jurisdição ressalta ser a garantia de existência do Estado Democrático de Direito, a permanência e a manutenção do ordenamento jurídico, e a respeitabilidade à Constituição Federal no que concerne à obediência os seus princípios, valores e vontades.

4.2 Competência

A palavra competência tem várias vertentes, pode referir-se à aptidão, ao designar a qualidade de quem é capaz de resolver determinados problemas ou de exercer determinadas funções; à idoneidade, quando estamos perante um sujeito capaz de avaliar algo ou alguém.

No Direito, a competência é a atribuição jurídica outorgada a certos órgãos do Estado de uma jurisdição relativamente a determinadas pretensões processuais com preferência aos demais órgãos da sua classe. É, portanto, um conjunto de regras que estabelecem qual o tribunal que deve julgar uma causa.

O art. 5º, inc. LIII da Constituição Federal, nos traz como a jurisdição é distribuída por leis nos órgãos de poder judiciário fazendo uma repartição de competências. Vejamos:

> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> LIII. ninguém será processado nem sentenciado senão pela autoridade competente; (BRASIL, 2021).

A lei penal no espaço abrange um território não delimitado que pode ser físico ou virtual, o que dificulta a delimitação da área Penal para a aplicação da lei. O espaço virtual traz uma facilidade de interação com diversos países transpondo barreiras físicas com o único meio em comum a rede.

Ao imaginar a possibilidade de a rede ser um território onde se encontra a informação, não se tem algo preciso, já que ela pode ser conectada de qualquer lugar, o usuário pode se utilizar da identidade que desejar e o controle quanto à identificação não é necessariamente pessoal, gerando ainda mais dificuldade para sua localização como exemplificado na possibilidade de se acessar um computador brasileiro com um IP estrangeiro de forma a ser identificado erroneamente, gerando assim uma barreira para distinção da competência entre os Estados e consequentemente a inexatidão quanto a identidade do criminoso.

Entretanto, não há que se mensurar delimitação do espaço cibernético, pois é certo que cada país possui sua soberania e jurisdição, temos, portanto, um primeiro aspecto que demonstra a complexidade do crime virtual.

Quando se fala em conceito de espaço já surge dúvida em relação à eficácia da lei penal no espaço, no ordenamento jurídico brasileiro existem princípios norteadores a esse respeito elencados.

4.3 Princípio da Territorialidade

De acordo com o princípio da territorialidade, a lei aplicável é a do local do ato praticado, e este princípio se sujeita à lei processual do lugar do crime onde o juiz exerce a jurisdição, não só aos nacionais, como também os estrangeiros domiciliados nos país.

No Brasil adota-se a teoria da ubiquidade, prevista no Código Penal, considerando o local da conduta, ação, omissão ou o local do resultado da ação criminosa.

Quando aplica esse princípio à prática dos crimes virtuais, fica simples no caso em que o fato cometido no Brasil seja tipificado como ilícito, pois mesmo praticado pela internet deve ser repreendido. Ocorre que o ambiente virtual não tem fronteiras, ocorrendo casos em que resultado é típico no país em que o comando é dado, porém atípica no Estado onde ocorra o resultado fático.

Na busca da resolução para o conflito leva-se em consideração que as normas de caráter penal são interpretadas restritivamente cabendo ao aplicador optar pela que seja menos prejudicial ao réu, levando em consideração, tratados e legislação especifica nos países envolvidos.

No Brasil, há a possibilidade de aplicação da lei penal fora de seu território, inclusive no território por extensão, mas apenas para infrações cometidas em seu território, conforme previsão no artigo 5º, caput, do Código Penal Brasileiro. “Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional”.

Nesse raciocínio quanto à lei penal brasileira no espaço será aplicada quando qualquer fato tipificado atinja o território brasileiro, então a lei alcançará o fato regido.

4.4 Princípio da Extraterritorialidade

Já para alguns casos específicos, a lei brasileira pode também ser aplicada fora do território, como já mencionado, em casos previstos e norteados por princípios previstos na Carta Magna, que dispõe sobre o princípio da defesa a proteção real prevista no artigo 7º, inciso I, §3º que a lei aplicada é a que se refere à nacionalidade do bem jurídico lesado. Apesar da possibilidade de punibilidade e aplicação Brasileira nos casos previstos é evidente que não há facilidade em executar as leis já que cada país possui suas próprias leis.

5 LEGISLAÇÃO

Nos regimes democráticos, três poderes apresentam-se bem definidos e atuantes: o Poder Executivo, o Poder Legislativo e o Poder Judiciário. Quanto ao Poder Legislativo, a ele compete produzir e manter o sistema normativo, ou seja, o conjunto de leis que asseguram a soberania da justiça para todos – cidadãos, instituições públicas e empresas privadas.

Em resumo, a legislação de um estado democrático de direito é originária de processo legislativo que constrói, a partir de uma sucessão de atos, fatos e decisões políticas, econômicas e sociais, um conjunto de leis com valor jurídico, nos planos nacional e internacional, para assegurar estabilidade governamental e segurança jurídica às relações sociais entre cidadãos, instituições e empresas.

Apesar da omissão no nosso ordenamento jurídico e com todas precariedades que norteiam o assunto em questão, os crimes virtuais praticados no Brasil são punidos, pois, mesmo que as condutas não sejam totalmente tipificadas, alguns dos crimes que são cometidos no âmbito virtual já são previstos no Código Penal, não permitindo que essas condutas passem despercebidas aos olhos da justiça e da sociedade, pelo menos em tese.

A Constituição Federal de 1988 em seu art. 5º, inc. XXXIX dispõe:

> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> XXXIX – não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. (BRASIL, 2021).

Nesse sentido, faz-se entender que para que se venha a punir aqueles que cometem os crimes virtuais, dos quais não são tipificados em nosso ordenamento jurídico, é necessário a adequação às normas que já existem, e que as lacunas que ainda existem devem ser preenchidas, e hoje, mais do que nunca é necessário que haja a incorporação dos conceitos de informática em relação à nossa legislação vigente.

5.1 Lei 12.737/12 “Lei Carolina Dieckmann”

A Lei nº 12.737, de 30 de novembro de 2012, altera o Código Penal, trazendo a tipificação criminal que chamamos de crimes virtuais. Esta lei tipificou como crime a invasão de dispositivo informático, criminalização ocasionada com a atriz Carolina Dieckmann, que teve seu computador invadido e todos os seus arquivos pessoais subtraídos e sendo expostas suas fotos íntimas nas redes.

Há que se mencionar que embora a lei tenha sido um marco, foi elaborada em regime de urgência, isso quer dizer que, o direito penal foi utilizado como mecanismo para aplacar a comoção popular, isso gerou bastante críticas.

No meio da modernização da legislação criminal, o art. 154-A do Código Penal (2012) tipifica o comportamento daquele que invade 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 vulnerabilidade para obter vantagem ilícita. Vejamos:

> 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 vulnerabilidade 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 de conduta definida no caput.
> ...
> § 3º Se da invasão resultar a obter de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crimes mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade de o crime for praticado contra:
> I – Presidente da República, governadores e prefeitos;
> II – Presidente do Supremo Tribunal Federal;
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou Câmara Municipal; ou
> IV – Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 2021).

O objeto jurídico do crime é a privacidade individual ou profissional, que está armazenada em dispositivo informático, desdobramento lógico do direito fundamental

assegurado no art. 5º, X, CF/88, dizendo que: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito de indenização pelo dano material ou moral decorrente de sua violação.”

Além disso, o termo “dispositivo informático” também foi criticado pelo fato de que seria melhor ter sido utilizado o termo “dispositivo eletrônico” para abranger a alta quantidade de aparelhos que possuem acesso à internet, como celulares, smartphones, televisores, etc.

Dito isto, a lei tem se revelado insuficiente para repreender os crimes dessa natureza, por não tipificar todas as condutas possíveis além da existência das lacunas na parte que já está tipificado.

5.2 Lei 12.965/14 “Marco Civil da Internet”

O Marco Civil da Internet surgiu com o apelido de “constituição da internet”, pois passou a ter uma normatização dos direitos, garantias e deveres de usuários e provedores de internet no país, foi erguida pelos princípios da Neutralidade de Rede, a Liberdade de Expressão e a Garantia da Privacidade.

Possui 32 artigos que tratam sobre temas como os direitos e garantias dos usuários, a provisão de conexão e aplicações da Internet, a responsabilidade dos provedores, a atuação do poder público, entre outros.

Vejamos alguns e importantes artigos que versam sobre o tema:

> Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.
> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I - o reconhecimento da escala mundial da rede;
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III - a pluralidade e a diversidade;
> IV - a abertura e a colaboração;
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI - a finalidade social da rede.
> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.
> Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
> I - do direito de acesso à internet a todos;
> II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
> III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
> IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.
> Art. 5º Para os efeitos desta Lei, considera-se:
> I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
> II - terminal: o computador ou qualquer dispositivo que se conecte à internet;
> III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
> IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
> V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP. (BRASIL, 2021).

O Marco Civil se tornou um exemplo mundial de regulamentação da internet, tanto para usuários quanto para os provedores, tendo inclusive influenciado a criação de Leis em países como a França e Itália. Cita ainda COSTA, que:

> Em que pesem as críticas, o Marco Civil da Internet recebeu elogios de autoridades no assunto - como os fundadores do world *wild web,* Tim Berners-Lee e Vint Cerf - e serviu de inspiração para outros países – como a Itália e a França – criarem suas legislações. A norma brasileira é considerada um modelo para organizações como o Fórum Econômico Mundial e a Corporação da Internet para Atribuição de Nomes e Números 6 (2016, texto digital).

Um dos fatos marcantes que surgiram com o Marco Civil da internet, foi a retirada do conteúdo, que veio para garantir direitos, uma vez que seja ofendido, com

violação de intimidade, o ofendido pode solicitar a retirada do conteúdo. Conforme expõe o art. 19 da Lei nº 12.965:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
> § 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.
> § 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.
> § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.
> § 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação. (BRASIL, 2021).

Apesar de o Marco Civil ser uma lei muito elogiada, a nível mundial, por garantir direitos e deveres aos usuários, bem como aos provedores e fornecedores de internet no país, ainda apresenta alguns desafios para ser mais conhecida pela população brasileira, mesmo com cada vez mais usuários no território nacional e havendo uma maior facilidade de acesso à informação, justamente pelo meio online, ela ainda não é de conhecimento de todos.

5.3 Código Civil e as punições previstas para os crimes virtuais

Cesare Beccaria, em sua obra “Dos Delitos e das Penas” nos traz a seguinte reflexão acerca das penas:

> O rigor das penas deve ser relativo ao estado atual da nação. São necessárias impressões fortes e sensíveis para impressionar o espírito grosseiro de um povo que sai do estado selvagem. (2001, p.21).

Dito isto, ele (Beccaria) quis dizer que as penas, aliás, os crimes devem ser punidos com penas que estejam em consonância com a realidade da sociedade,

então, se os crimes cibernéticos tiveram um imenso aumento, um dos fatores que fomentam esse crescimento, está relacionado com a regulamentação adequada para enquadrar esses delitos.

Como podemos ver nesse trecho por Eugênio Raúl Zaffaroni:

> “A efetividade do direito penal é a sua capacidade para desempenhara função que lhe incumbe no atual estágio de nossa cultura. (...) um direito penal que não tenha esta capacidade será não efetivo e gerara tensões sociais e conflitos que acabarão destruindo sua eficácia (vigência).” (2004, n.p.)

O Brasil conta com aproximadamente 11 delegacias que tratam sobre os crimes virtuais, e elas são somente nos maiores centros do país, se tratando de um lugar que direto vem a ser alvos de ataques virtuais, é muito pouco.

Por meio dessas Delegacias Especializadas é possível fazer o boletim de ocorrência dos delitos ocorridos na internet, sendo os mais comuns os crimes de calúnia, difamação, injúria, estelionato, dano e violação de direitos autoriais. Essas delegacias também têm efetuado os inquéritos relativos aos crimes de informática.

Dito isto, o nosso Código Civil, diante da falta da tipificação legal desses crimes virtuais, nos traz a possibilidade de reparação monetária que visam suprir os danos sofridos pelas vítimas, sejam eles morais ou materiais. Vejamos os seguintes artigos do Código Civil de 2002:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.
> ...
> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. (BRASIL, 2021).

Os danos morais são aqueles relativos à moral de uma pessoa, que estão ligados à sua intimidade, sua honra, sua dignidade, ou seja, todos aqueles danos que uma pessoa sofre na sua esfera íntima, que repercutem direto na sua saúde física e psíquica.

Já os danos materiais, como o nome sugere, diz respeito aos bens materiais de uma pessoa, de modo geral, ou seja, são todos aqueles danos que alguém sofre em seu patrimônio.

Nos Crimes virtuais a maioria dos crimes estão ligados aos danos morais ou materiais, tanto que a Lei Carolina Dieckmann foi criada exatamente por ferir a privacidade da atora com intuito exatamente de ter uma vantagem em cima disso, neste caso especifico ele cometeu os dois danos.

CONSIDERAÇÕES FINAIS

Como foi aludido, é inegável as inúmeras facilidades que a internet trouxe para a sociedade, seja na área política, econômica, social ou cultural. Mas como toda coisa tem seu lado positivo, também tem o lado negativo, que no caso são os crimes virtuais, que são inúmeros, como: crimes contra a honra, pornografia infantil, da prática de racismo e de fraudes em contratos eletrônicos, dentre outros.

Diante dessa proliferação dos chamados crimes cibernéticos é que surge o Direito Digital, com intuito de evoluir a própria ciência jurídica, abrangendo todos os princípios fundamentais e institutos do Direito vigente. Para combater os crimes virtuais, surgiram legislações, como a Lei Carolina Dieckmann, Marco Civil da Internet, afim de impedir ou pelo menos controlar esses delitos, porém, um dos grandes empecilhos e, que no fim, acaba fomentando a impunidade é a falta, ainda, de normas específicas de regulamentação dos ilícitos nesse mundo virtual. A legislação nacional demonstrou alguns avanços, todavia, ainda é uma legislação tímida, carente de uma melhor regulamentação e maior precisão técnica, a fim de criar tipos penais específicos aos crimes virtuais para evitar que haja impunidade dos agentes.

A mera elaboração de norma, ou de normas, ainda não é o suficiente para combater esses delitos, o Estado com seu papel regularizador, precisa também adotar outras medidas, como: conscientização da população acerca desses crimes, implementar mais conteúdos que eduquem as crianças e adolescentes nas escolas e também esse tema merece uma maior atenção pelas autoridades pois os números dos aumentos desses crimes são assustadores, mostrado por diversas pesquisas. Com a legislação que temos, algumas condutas conseguem ser abarcadas, mas outras ainda carecem de projetos de lei, ou seja, O Direito deve acompanhar a evolução da sociedade para que não fique inseguro a utilização dos meios eletrônicos no dia a dia.

Dito isto, as legislações, doutrinas e jurisprudências que surgirão no decorrer dos anos, devem procurar se adequar a essa realidade de maneira proporcional, pois não adianta nada só aumentar as penas se não temos delegacias especializadas para que garanta o funcionamento e patrulhamento desses crimes no mundo virtual. Urge a necessidade de que os órgãos responsáveis pela persecução penal, como as Polícias Civil e Federal, bem como o Poder Judiciário e o Ministério Público, instruam

seus agentes acerca das infinitas possibilidades trazidas pelo uso da internet e, consequentemente, das ameaças que nela estão presentes. É necessário a capacitação técnica especifica, para que estejam preparados para lidar com as inúmeras adversidades e situações. Devendo proporcionar instrumentos de trabalhos compatíveis com a nova realidade criminosa.

Por fim, é inegável a necessidade de criação de leis especificas que completem o ordenamento jurídico, ainda mais pela ambiguidade e falta de suporte que os operadores do Direito têm em julgar ações delituosas o que acaba por não promover a justiça. Então, é necessário que o Governo adote políticas públicas no sentido de conscientizar a comunidade em geral acerca do uso correto dos serviços disponíveis na internet, assim dificultaria a ação dos criminosos, diminuindo a possibilidade de sucesso das investidas dos mesmos, pois a prevenção é, sem dúvidas, uma das medidas mais eficientes.

REFÊRENCIAS

BRASIL, **CÓDIGO CIVIL 2002.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>. Acesso em: 14.05.2021

BRASIL, **CONSTITUIÇÃO FEDERAL 1988.** Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 14.05.2021

BRASIL, **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 14.05.2021

BRASIL, **LEI Nº 12.965, DE 23 DE ABRIL DE 2014.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 14.05.2021

BECCARIA, Cesare. **Dos delitos e das penas.** (2001) Ridendo Castigat Mores (Versão para ebooks) disponível em: < http://www.ebooksbrasil.org/adobeebook/delitosB.pdf> Acesso em: 18 setembro 2021.

BERGMAN, apud Pompéo, Wagner Augusto; Seefeldt, João Pedro. **Nem tudo está no Google: deep web e o perigo da invisibilidade.** In: Congresso Internacional de Direito e Contemporaneidade. Santa Maria: UFSM, 2013, p. 441.

CANAL TECH, 2019. **O que são crackers e hackers?** Disponível em: https://canaltech.com.br/seguranca/o-que-e-cracker-hacker-diferenca/> Acesso em: 14.05.2021

CASTRO, C. R. A. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

CONJUR, Consultor Jurídico. **STJ lança estudo que reúne 65 julgamentos de crimes virtuais contra a honra.** Disponível em: www.conjur.com.br/2015-out-07/stj-lanca-estudo-reune-65-julgamentos-crimes-internet. Acesso em: 20 de setembro de 2021.

CONVENÇÃO DE BUDAPESTE. **Convenção Sobre Cibercrime.** Disponível em:http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_Portugese.pdf > Acesso em 14.05.2021

COSTA, Thabata Filizola, **A importância do Marco Civil da Internet: Lei 12.965**, Jusbrasil/artigos, 2016. Acesso em: 18 de setembro de 2021.

COSTA, M. A. R. **Crimes de informática**. Disponível em: <https://jus.com.br/artigos/1826/crimes-de-informatica >. Acesso em: 05 novembro de 2021.

CHAWKI, Mohamed; WAHABI, Mohamed. **Identity theft in cyberspace**: issues and solutions. Disponível em:. Acesso em: 14.05.2021.

DICIO, **Dicionário Online de Português.** Disponível em: https://www.dicio.com.br/ubi-societas-ibi-jus. Acesso em: 14.05.2021

DIGITAL, Cultura. **Marco Civil da Internet: seus direitos e deveres em discussão.** Disponível em: http://culturadigital.br/marcocivil/>. Acesso em: 14.05.2021

FELICIANO, Guilherme Guimarães. Informática e criminalidade. Parte I: lineamentos e definições. **Boletim do Instituto Manoel Pedro Pimentel**, São Paulo, v. 13, n. 2, p. 35-45, set. 2000. p. 42.

FERNANDO JI HOON YU, 2020. Disponível em: https://jus.com.br/artigos/81817/deep-web-analise-acerca-do-crime-envolvendo-pedofilia-na-internet> Acesso em: 14 de setembro de 2021.

FERREIRA, I. S. (2005). **Direito & Internet: aspectos jurídicos relevantes**. 2 ed. São Paulo: Quartier Latin.

JESUS, Damásio E. de. **Direito Penal:** parte especial. 22 ed. Revista e atualizada. São Paulo, Saraiva, 1999, 2v.

MINISTÉRIO PÚBLICO FEDERAL. **Crimes cibernéticos**: Manual Prático de Investigação. Disponível em: <https://www2.mppa.mp.br/sistemas/gcsubsites/upload/60/ManuaL%20Pr%C3%83%C2%A1tico%20de%20Investiga%C3%83%C2%A7%C3%83%C2%A3o%20sobre%20Crimes%20de%20Inform%C3%83%C2%A1tica.PDF>. Acesso em: 14.05.2021

NACIONAL, LINK. **HISTÓRIA DA INTERNET**: veja como evoluiu até hoje. Disponível em: https://www.linknacional.com.br/blog/historia-da-internet/> Acesso em: 14.05.2021

NEGOCIOS, EPOCA. **GOLPES VIRTUAIS DISPARAM COM COVID 19** (Disponível em: https://epocanegocios.globo.com/Brasil/noticia/2020/06/epoca-negocios-golpes-virtuais-disparam-com-covid-19.html. Acesso em 14.05.2021)

PINHEIRO, Patrícia Peck. Direito Digital. 4ed. Ver., atual. eampl. São Paulo: Saraiva, 2011.

PINHEIRO, R. C. **Os cybercrimes na esfera jurídica brasileira**. Disponível em: <http://jus.com.br/revista/texto/1830/os-cybercrimes-na-esfera-juridica-brasileira>. Acesso em: 05 de novembro de 2021.

REALE, Miguel. **Lições Premilinares de Direito**. 27. ed. São Paulo: Saraiva, 2002. p. 2

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. São Paulo, Memória Jurídica, 2004.

SILVA, Ana Karolina Calado da. **O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca de sua produção probatória em contraponto à jurisprudência contemporânea brasileira**. Portal de e-governo, inclusão digital e sociedade do conhecimento: 06/04/2015. Disponível em: Acesso em: 20 de setembro de 2021.

TECH TUDO, 2019. **O que é Deep Web?** Disponível em: https://www.techtudo.com.br/noticias/2019/03/o-que-e-deep-web.ghtml> Acesso em: 15.04.2021

ZAFFARONI, Eugênio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro** – Parte Geral. São Paulo: editora Revista dos Tribunais, 2004.