Revista Ibero- Americana de Humanidades, Ciências e Educação- REASE

OPEN ACCESS

doi.org/ 10.51891/rease.v7i10.2684

CRIMES VIRTUAIS: LEGISLAÇÕES INSUFICIENTES OU INEFICIÊNCIA DAS AUTORIDADES COMPETENTES?

Ariovaldo Nascimento Ribeiro Reis[1]
Geraldo Denison Viana[2]

RESUMO: Este artigo apresenta noções gerais relacionadas aos crimes virtuais, composto pelos conceitos mais utilizados, bem como os tipos mais comuns destes crimes ocorridos no mundo afora, legislações e a proposta reconhecida como mais coerente para o combate desses delitos.

Palavras-chave: Crimes virtuais. Conceito. Legislações. Proposta.

ABSTRACT: This article presents general notions related to cyber crimes, composed of the most used concepts, as well as the most common types of these crimes occurring worldwide, legislation and the proposal recognized as the most coherent to combat these crimes.

Keywords: Cyber Crime. Concept. Legislation. Proposal.

1 INTRODUÇÃO

Ao decorrer das décadas é clara a necessidade humana de obter avanços tecnológicos direcionados aos diversos pontos da sociedade, buscando evoluções significativas voltadas à segurança, à saúde, à educação, à comunicação, aos comércios e ao entretenimento. Partindo do notório conhecimento quanto as comunicações, fica evidente o salto quântico relacionado a tal.

A aproximados 15.000 a.C, a humanidade tinha como forma mais eficaz de comunicação as chamadas pinturas rupestres (artes e desenhos feitos nos interiores das cavernas). Nos tempos atuais, em menos de um segundo conseguimos estabelecer uma comunicação estabilizada e eficaz, com raciocínio e diálogo lógico junto a alguém do outro lado do mundo, sem contar aos grupos em redes sociais e aplicativos de conversa, onde há a possibilidade de inserir diversas pessoas de todos os cantos do planeta contendo a mesma velocidade e eficácia em suas comunicações (existindo não só avanços como estes mas milhares de outros significativos para as nações).

[1] Graduando do Curso de Direito – **Faculdade Pio Décimo** – Aracaju/SE. E-mail: arireisneto@hotmail.com/arinr.reis@outlook.com
[2] Professor Mestre em Direito – Faculdade Pio Décimo / Aracaju-SE

O presente artigo tem o intuito de esclarecer acerca das dúvidas existentes quanto aos conceitos dos crimes cibernéticos desmistificados e unificados por alguns doutrinadores (tais questionamentos direcionados aos crimes virtuais puros, mistos e comuns), bem como citar os tipos de crimes virtuais mais evidentes e ocorrentes em nossa sociedade contemporânea. Além do disposto anteriormente, analisaremos também acerca das legislações atuais, das que se propuseram a ser eficaz no teórico mas na prática torna-se uma realidade totalmente diversa.

Percebe-se que no Brasil há uma enorme deficiência destinada à tentativa de prevenir as ocorrências e existências dos mais diversos crimes no meio virtual, seja pela ineficiência das legislações específicas e as que se podem fazer interpretações extensivas ou por analogia, seja pelas políticas públicas, investigações e agentes não tão bem destinados e treinados para delitos existentes no mundo cibernético. Analisaremos acerca da proposta intencionada à propositura de um método mais eficiente intencionado aos agentes investigativos (não só no Brasil já que esses tipos de condutas ilícitas e delituosas não apenas o afeta) em diversas nações.

Utilizaremos também como arcabouço base para a continuidade e propulsão das pesquisas relacionadas ao tema, diversos artigos científicos muito bem elaborados e destinados à tentativa da formação de uma compreensão mais concreta, bem como monografias e livros dos mais diversos autores especializados no tema. A legislação mais conhecida no Brasil e que aborde os crimes ocorridos no ambiente virtual é a lei nº 12.737/2012 (apelidada de lei Carolina Dieckmann) surgiu como uma tentativa de desacelerar ou abolir completamente da nossa sociedade os crimes virtuais, bem como a tentativa de punir os infratores destes. Existente também a lei nº 12.965/2014 (apelidada como lei do Marco Civil da Internet) onde disciplina as garantias e direitos referentes ao uso da internet no Brasil.

Ao analisar, além do já supracitado, alguns dados estatísticos referentes aos crimes virtuais ocorridos no Brasil, tais como os *phishing* por exemplo, constatará que houve uma larga escala de delitos consumados em períodos eleitorais bem como em épocas de grande comoção internacional (a exemplo disto, a Copa do Mundo).

Portanto, a intenção do presente artigo é informar acerca dos diversos crimes virtuais, bem como suas legislações e estatísticas sobre tais delitos formando assim um raciocínio objetivando uma melhor compreensão do mundo cibernético, objetivando uma ponte para a

crucial e repentina pergunta referente ao tema: Crimes Virtuais, legislações insuficientes ou ineficiência das autoridades competentes?

2 FUNDAMENTAÇÃO TEÓRICA

Com o passar das décadas fica clara a importância da tecnologia em nosso mundo contemporâneo. Em diversos pontos da sociedade a informática desenvolveu-se exponencialmente apresentando evoluções cruciais, a exemplo disto estão fatores evidentes no ramo da saúde, comércio e entretenimento. A tecnologia teve o seu maior avanço já feito com a criação da internet (um grande passo na revolução digital) ferramenta esta de suma importância (imensamente utilizada para a difusão de conteúdos em geral) ao prosseguimento da globalização. Percebe-se assim que o acesso às informações pela internet tornou-se algo costumeiro e de alcance descomunal onde engloba-se também os contatos entre pessoas mundo afora, alcançando assim o patamar de uma das invenções mais importantes da contemporaneidade.

Partindo da observação do senso comum relacionado à internet, entende-se que há diversos fatores positivos contribuintes com as nações, porém seria claro que haveria a tentativa dos criminosos em aproveitar-se desse meio para a consumação de delitos, havendo assim a expansão de diversos fatores negativos. Assim que houve o surgimento desses delitos virtuais, as comunidades ao redor do mundo necessitaram de normas e legislações (aqui no Brasil temos a lei nº 12.737/2012) que regulamentem o uso do meio cibernético (antes considerada, e por muitos, como "terra de ninguém").

A lei nº 12.737/2012 (apelidada de Lei Carolina Dieckmann) é um marco muito importante na legislação brasileira voltada para os crimes virtuais. Tendo como válvula propulsora a infelicidade ocorrida com a atriz brasileira de mesmo nome, é a legislação reconhecida como a principal para o combate dos crimes do mundo cibernético, porém a norma apresenta várias lacunas que causam prejuízos na tentativa de prevenção e combate aos atos ilícitos, tudo isso consequência da celeridade em que a norma foi criada. Na época da criação desta legislação, houve uma enorme pressão ao Congresso Nacional para a elaboração de uma norma que abordasse sobre os crimes cibernéticos/virtuais em si, pela falta de controle da quantidade de crimes virtuais existentes e a falta de punição aos seus infratores. Apesar de o Brasil ter essa legislação vista como central quando trata-se de crimes virtuais, muitos teóricos,

juristas, doutrinadores e profissionais do ramo do direito a reconhecem como ineficaz ao combate e punição dos criminosos, uma vez que existem diversas lacunas e várias "portas" de entrada para diversas interpretações.

A amplitude e diversidade de crimes que podem ser cometidos no mundo virtual existe de forma avassaladora, sendo os crimes mais comuns os de estelionato virtual, invasão de informações particulares ou secretas, pornografia infantil, tráfico, *cyberbullying*, ofensas à dignidade sexual e à honra da vítima, abusos nos atos de *sexting* (mal apelidada de pornografia da vingança, ou *revenge porn*), *phishing*, dentre outros.

Há de se perceber que partindo do ponto de referência da tentativa de prevenção e para uma investigação mais incisiva e eficaz quanto aos crimes cibernéticos, deve-se haver uma cooperação e contribuição de todos os pontos da sociedade (não só nacionais mas também uma união entre as nações mundo afora), principalmente das entidades públicas e privadas. É notório que na atual sociedade brasileira há uma necessidade maior de mudanças direcionadas às normas jurídicas pois é clara a impossibilidade de manter as atuais para investigação dos crimes cibernéticos (sendo a principal e também não tão eficaz quanto se propusera a ser, a lei Carolina Dieckmann nº 12.737/2012) já que a legislação vigente deixa diversas brechas, bem, como penas brandas que dificultam a punibilidade do criminoso, além das dificuldades na retirada dos conteúdos ilícitos do arcabouço virtual.

Em meio à grande massa de crimes existentes e potencializados por meio da informática, tais como os crimes já supracitados contra a dignidade sexual e intimidade, contra a honra (calúnia, injúria e difamação), crimes de ameaça e falsa identidade, as práticas de '*sexting*' como meio para ofender a imagem da vítima, ciberterrorismo e fraudes eletrônicas, surgiu também um novo tipo de crime que é de ação bastante comum nos meios atuais, nomeado de '*formjacking*'. Os ataques do '*formjacking*' são simples (muitas vezes lembrados com ataques aos caixas eletrônicos), sendo o envio de códigos maliciosos em sites de lojas virtuais, no intuito de extrair informações pessoais e financeiras dos clientes. Os danos não são direcionados apenas aos clientes dessas lojas virtuais (parte mais vulnerável pois não terão noção nenhuma se o site em que estão deixando informações essenciais, tanto pessoais quanto financeiras, está infectado com os '*formjacking*' ou não) mas também à própria empresa, como consequência principal os pontos negativos direcionados à imagem e reputação das mesmas, além do dano financeiro decorrente.

Diante dos fatos anteriormente citados relacionados aos cibercrimes, sendo o conjunto de crimes concretizados pela utilização de meios informáticos/tecnológicos, há de se notar que os mesmos já foram datados em 1960, tendo como práticas que encaixavam-se nas características do estelionato. Uma das principais características dos cibercrimes é que por serem feitos em um ambiente não físico (virtual por assim dizer), eles tornam-se muito voláteis (por exemplo, os autores dos crimes podem agir em outro país) podendo ser facilmente alterados e apagados, sendo assim de extrema dificuldade o rastreamento de sua real autoria, da sua consumação, já que um simples desligar de um computador, por exemplo, pode encerrar os meios de investigação dos pontos cruciais e fundamentais para a designação do seu real autor e responsável. Na grande maioria das vezes algumas informações relacionadas ao crime ocorrido são resgatadas mas as investigações encerram-se no meio do caminho pelo simples fato de que não conseguem encontrar informações hábeis ou cruciais para encontrar a materialidade e sua autoria. Para ter um pouco em mente da dificuldade notória de materializar um crime virtual, pode-se perceber que existirá uma reverberação jurídica nos casos em que, o crime tenha sido feito no país "A", onde o autor do crime esteja no país "B" e o objeto do fato criminoso esteja no país "C".

Além dos cibercrimes terem o conceito já anteriormente citado, há também o reconhecimento dos mesmos como "ações prejudiciais atípicas", sendo entendida como as ações que por mais causadora de dano e prejuízo que sejam, não poderão ser reconhecidas nem responsabilizadas como crime, pelo simples fato da não tipificação da conduta nas legislações (por exemplo, um indivíduo que invada o computador de um conhecido sem ter o objetivo de obter, alterar ou excluir dados ou informações ou sem violar algum mecanismo de segurança, este indivíduo não será indiciado nem preso, já que esses fatos não serão considerados condutas criminosas, portanto não se encaixariam no artigo 154-A do Código Penal).

Percebe-se assim que a discussão vai mais além do que é percebida. Há diversos fatores que estão interligados e que geram receios e inseguranças (as investigações ineficazes, a impunidade e não responsabilização dos criminosos). Além das modificações legislativas existentes e pretendentes, há de haver a criação de órgãos mais especializados nessas determinadas áreas de atuação. No Brasil, apesar da grande incidência de crimes cibernéticos já que os lucros havidos dessas condutas superam os lucros do tráfico de drogas, já existem pontos

na legislação que cobrem e preveem diversas dessas atitudes como ilícitas e típicas de responsabilização penal e cível. Porém, o que deve ser observado são as novas práticas que surgem a cada dia e diversidades das que já existem, sendo o maior desafio aos profissionais.

Portanto, levando isso como ponto fundamental para uma futura prevenção dos crimes ocorridos no meio virtual, há de existir uma cooperação entre todas as entidades (públicas e privadas) e a sociedade pois, nesses atos criminosos o elo mais fraco é a vítima que não detém conhecimento para prevenção e age na grande maioria das vezes de forma negligente, tornando assim seu próprio sistema, bem como os demais, vulneráveis.

3 Crimes Cibernéticos ou Cybercrimes

É inquestionável o fato da ascendência dos crimes em todo o mundo havendo como simples fato da existência de inúmeros meios para a realização e consumação dos delitos. Dentre os meios mais populares, existe a Internet. Percebe-se então que a internet virou um dos maiores meios para a concretização dos crimes e contravenções existentes e respaldadas em nossa legislação, tendo como base as informações citadas pela Polícia Federal que constatou a fraude digital como o segundo maior crime lucrador realizado no Brasil, perdendo apenas para o tráfico de drogas (em 2019, o site de notícias "O Tempo" publicou uma matéria no dia 06 de setembro relacionada à Fraude Digital onde, no período de 12 meses que encerrava-se em agosto deste mesmo ano, mais de 12 milhões de consumidores foram alvos das fraudes, gerando um prejuízo de R$ 1,8 Bilhão).

Os crimes cibernéticos vistos como crimes bastantes voláteis, mais popularmente conhecido como crimes virtuais ou cybercrimes, são de forma geral os crimes que utilizam como meio para concretização do ato delituoso instrumentos tecnológicos tais como computadores, *smartphones*, aplicativos em ambas as plataformas, dentre outros. Segundo Renata da Silva Carvalho, a conceituação mais direta aos crimes cibernéticos é que "Os Crimes Digitais, conhecidos como Crimes Cibernéticos ou Crimes de Alta Tecnologia, representam as condutas criminosas cometidas com o uso das tecnologias de informação e comunicação, e também os crimes nos quais o objeto da ação criminosa é o próprio sistema informático" (CARVALHO, s/d, online). Segundo Paulo Marco Ferreira Lima (2012, online), os crimes cometidos no ambiente virtual podem ser conceituados como:

> Crimes de computador são qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina

> computadorizada tenha sido utilizada e, de alguma forma, tenha facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o autor ou que, pelo contrário, produza um benefício ilícito a seu autor embora não prejudique de forma direta ou indireta à vítima." (LIMA, s/d, online).

A sua nocividade é elevada e alguns atingem diversos pontos da população de maneira desenfreada uma vez que tenham sido cometidos, pois por serem atos delituosos cometidos em um ambiente fora do mundo real, ou seja, no mundo virtual, dificilmente consegue-se identificar e punir o autor do delito, onde na grande maioria dos casos esses criminosos saem impunes e estão livres para cometer outros atos delituosos.

Visto a conceituação básica e mais comum dos crimes virtuais, há de se observar também as denominações dadas por Ferreira e Crespo, onde entendem que existem apenas duas classificações para os crimes cometidos no ambiente virtual, sendo elas denominadas de crimes virtuais ou informáticos próprios e impróprios.

Os crimes informáticos próprios (ou puros) são aqueles que precisam necessariamente da existência do instrumento tecnológico para existir, caso contrário o crime não ocorrerá ('*formjacking*' por exemplo, sendo resumidamente quando os criminosos inserem códigos maliciosos em sites de lojas para extrair dados de contas dos clientes). Já os crimes informáticos impróprios (impuros) são aqueles, contrariamente aos crimes informáticos próprios, que não necessitam ou não dependem exclusivamente do meio informático pra serem concretizados pois já estão tipificados no código penal, porém a tecnologia é o meio utilizado para a execução destes crimes, tendo como exemplo a pornografia infantil (compartilhamento de fotos e/ou vídeos, por exemplo), estelionato, induzimento e instigação ou auxílio ao suicídio, ameaça dentre outros.

O surgimento da internet nos anos 1960, mais precisamente nos estudos e pesquisas militares no auge da Guerra Fria entre os EUA e a URSS, tinha como intuito inicial dela ser o meio de comunicação mais seguro da época, servindo de auxílio ao combate às guerras bem como servindo de servidor para base de dados governamentais e de segurança nacional. Sendo esta a intenção inicial, paralelamente começaram-se os usos indevidos desta tecnologia avançada (para a época), tendo como relatos iniciais as manipulações e sabotagens dos sistemas de computadores. Assim nasceram os crimes virtuais.

Segundo Roberto Chacon Albuquerque, em sua obra "A Criminalidade Informática", cita que:

> [...] os primeiros casos de crimes cibernéticos foram na década de sessenta. Eram utilizados computadores como forma de cometimento do crime virtual, como o estelionato. Na referida década foi que começaram a ser relatados pela imprensa os primeiros casos de crimes cibernéticos. A partir da década de setenta, começaram os primeiros estudos empíricos sobre a criminalidade cibernética.

Ao passar das décadas, engrenavam-se diversos avanços tecnológicos, chegando aos 1980, houve a ampliação da internet sendo utilizada para as relações comerciais, havendo deste modo a propagação dos crimes virtuais, tendo a pirataria, pornografia infantil, estelionato, vírus virtuais vistos como os principais crimes ocorridos na época. Daí surgiu a necessidade de reformular a segurança bem como os meios para conter os crimes cibernéticos e punir os infratores.

Eduardo Azeredo enquanto Deputado Federal, relatou no Senado um projeto de lei nomeado de PL 84/99 que dispunha sobre os crimes de clonagem de cartões de crédito e algumas disposições a respeito dos crimes informáticos, dentre outras denominações. Após tramitação, houve algumas alterações no texto do projeto de lei, onde em 2012 foi sancionada a Lei Azeredo (nº 12.735/2012). Após a aprovação da lei Azeredo, houve como base nesse texto a proposta da lei 12.737/2012, que modelou algumas alterações nas redações dos artigos 154-A, 154-B, 266 e 298 do Código Penal.

No Brasil, até a criação da lei 12.737/2012 apelidada de Lei Carolina Dieckmann (veio para integrar algumas modificações ao código penal no tocante dos crimes informáticos), não havia uma legislação específica que abordasse exclusivamente sobre os crimes no âmbito virtual (somente a singela lei Azeredo), onde o caso ocorrido com a famosa atriz deu-se o ponto de inicial ao incentivo para a confecção da lei. Muitos estudiosos, doutrinadores e advogados especialistas no tema a reconhecem como fraca e ineficaz, como se a mesma tivesse sido feita às pressas apenas ocasionando a falsa sensação de segurança perante os crimes virtuais, onde os seus dispositivos podem gerar dupla interpretação, além de serem amplos e confusos o quê facilitaria o enquadramento de condutas triviais e utilizações mais amplas para a defesa dos criminosos, tendo ainda penas não inibidoras, ou seja, não tão incisivas a ponto de fazer com que os meliantes cometessem novamente crimes.

Apesar das inúmeras críticas direcionadas à lei, deve-se entender que ela foi um dos primeiros passos para a tentativa de estabelecer um método que cessasse por completo os crimes virtuais em ascendência no país, pois demonstra também que o mundo virtual é um ambiente a ser organizado por um sistema jurídico prático e eficaz e não ser, como muitos até então achavam, ser uma "terra de ninguém", sem regras e regimentos que a organizem.

4 Tipos Mais Comuns dos Crimes Cibernéticos

Percebe-se que com a conceituação do quê são os crimes informáticos e o quê é o ciberespaço - sendo o ambiente virtual ou "espaço constituído por usuários e infraestrutura de rede na Internet" (BOFF, Salete Oro; FORTES, Vinícius Borges, p. 63, 2016) – tende-se a ficar mais fácil identificar os crimes ocorridos no mundo cibernético. Nos primórdios da Internet, em meados do ano 1963, suas primeiras experiências existentes foram realizadas por conta da criação da *ARPNET (The Advanced Research Projects Agency Network)*, onde fora utilizada como meio de comunicação interna do Departamento de Defesa dos Estados Unidos durante a Guerra Fria, pois precisariam na época utilizar de um meio para comunicar-se cujo não houvesse a interceptação de informações essenciais por parte dos "inimigos". Ao passar das décadas, em meados de 1980 foi criada a famosa *World Wide Web*, ou como é mais conhecida, a "WWW", por um físico chamado Tim Bernes Lee.

Como é de se perceber, com a grande propagação da Internet à época promovendo diversos pontos positivos nas comunicações entre povos e nações, facilitando o comércio entre regiões e promovendo um longo alcance às informações, ficaria meio óbvio de entender que não tardaria a utilização desse meio eficaz para tantas ações como um meio também eficaz para a realização de atos ilícitos, como afirma Salete Oro Boff e Vinícius Borges:

> Com a evolução da tecnologia e dos recursos vinculados à rede mundial de computadores, a World Wide Web, ou Internet como ficou popularizada, é conveniente a reflexão quanto aos insumos contributivos à cultura, acesso e democratização da informação, valorização da diversidade e o processo de inclusão digital. Contudo, também é indispensável promover reflexões voltadas aos problemas jurídicos advindos da evolução tecnológica, sobretudo decorrentes da massificação do uso da Internet (BOFF, Salete Oro; FORTES, Vinícius Borges, p. 63, 2016).

Para que haja a tipificação dos atos delituosos como crimes, há de se observar o grau de lesividade do ato para com o particular, além da observação dos princípios e garantias resguardados pela Constituição Federal que foram lesados (como por exemplo a honra e a

imagem), deve-se observar também as redações dos artigos dos códigos Penal e Civil, pois na grande maioria dos casos, são estas legislações que serão utilizadas para enquadrar a ação delituosa como crime.

4.1 Falsidade Ideológica nas Redes Sociais

Com o desenvolvimento das redes sociais na Internet, onde são utilizadas além de um meio de comunicação entre a população, como também um acesso às informações pessoais de cada usuário pois na grande maioria destes, deixam seus perfis recheados de informações pessoais não essenciais e desnecessárias onde qualquer pessoa tem o acesso a essas características (dentro das políticas internas de cada rede social), surgiu um dos crimes mais difundidos da atualidade, sendo este nomeado de Falsidade Ideológica, como cita Arthur Egewarth em sua monografia, que a sua prática seria a criação de falsos perfis nas redes sociais utilizando informações já existentes de outras pessoas (nome, idade, gênero e até imagem) e se passando por ela:

> [...] Um dos crimes mais praticados da internet é o de falsidade ideológica. Nestes casos, os usuários comuns utilizam as redes sociais para criar uma identidade falsa, que são conhecidos como "fake". Os usuários roubam os dados pessoais (fotos, nomes, etc.) de outra pessoa e passam a se denominar e se colocar no lugar da outra pessoa [...] (EGEWARTH, Arthur, p. 13, 2019).

Esses atos são mais difundidos na rede social popular conhecida como *Instagram*, onde as pessoas batalham e prezam por números de seguidores, não se preocupando com as consequências para si e também para o real detentor das informações utilizadas ocasionadas por conta da criação destes perfis falsos.

4.2 Estelionato Virtual

Tipificado no Código Penal, mais precisamente na redação do artigo 171, prevê que estelionato caracteriza-se quando:

> Artigo 171 do Código Penal: 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 de 1 a 5 anos e multa.

Ocorre também com bastante frequência quando o criminoso utiliza, por exemplo, da criação de cópias de sites de compra onde o consumidor ingressa neste endereço virtual no intuito de adquirir algum produto, inserindo assim seus dados pessoas (como RG e CPF), e também seus dados financeiros (número de cartão de crédito e senha). Por fim, o consumidor

fora enganado pelo estelionatário, achando que estava acessando o real site da loja virtual quando na verdade caíra na armadilha do criminoso, onde este saíra na vantagem de ter conseguido os dados financeiros (neste caso, os danos patrimoniais ao consumidor são evidentes, pois além da compra que foi concluída, o estelionatário tem acesso aos dados bancários).

Como pode-se perceber, esse tipo de crime acontece a uma velocidade descomunal e claramente se torna mais volátil, pois ocorreu em um ambiente virtual onde torna-se mais difícil de identificar o criminoso e puni-lo pelos danos causados das suas ações.

4.3 Crimes Contra a Honra no Meio Virtual

No Código Penal, mais precisamente do artigo 138 ao 145 do capítulo V, trata diretamente dos crimes contra a honra (calúnia injúria e difamação). No meio virtual, esses tipos de crimes também são bastante comuns, mas são mais tratados como *cyberbullying*. Trata-se da mesma conduta tipificada nos respectivos artigos supracitados, porém por ser consumado no meio virtual, são reconhecidos como *cyberbullying* (este termo deriva da mescla das duas palavras em inglês, onde *cyber* advém de cibernético que significa algum instrumento relacionado à tecnologia e bullying, que advém de *bully*, onde seria aquela pessoa que maltrata ou violenta pessoas por motivos fúteis).

Esses crimes contra a honra ocorridos no meio virtual são mais recorrentes através de postagens em sites, chats de comunicação, telefones celulares e até nas redes sociais tendo como ofensas comuns tais como xingamentos, ofensas pessoas. Por mais que o *cyberbullying* não tenha contato com agressões físicas, entende-se que os seus danos são maiores que o *bully* por se tratar de agressões psicológicas, onde em casos extremos pode resultar danos físicos (tentativa de suicídio é a mais recorrente). Como cita Ângela Tereza LUCCHESI e Erika Fernanda Tangerino HERNANDEZ:

> O termo bullying tem origem na língua inglesa e se refere a bully, aquele indivíduo que "(...) maltrata ou violenta de forma constante outras pessoas por motivos supérfluos" (RODRIGUES, s/d, online). Já o cyberbullying trata da forma de agressão virtual, por meio de redes sociais, telefones celulares, entre outras mídias virtuais. Embora no cyberbullying as agressões não sejam físicas, as consequências são tão ou até mais graves que as praticadas no bullying, pois os

> abusos têm cunho psicológico, mas, em situações extremas, podem chegar ao dano físico.

Além dos termos já citados anteriormente, quando relaciona-se ao *cyberbullying* outros termos também têm grande presença no meio virtual, sendo o "*hater*", "*sexting*" e o "*revenge porn*".

O *hater*, que deriva-se do inglês cujo significado é "aquele que odeia", está relacionado às atitudes de pessoas que disseminam o ódio gratuito direcionado a outrém. Já o *sexting*, pratica mais realizada ao público mais jovem, se consiste na prática de trocar mensagens que tenha como relação assuntos de caráter sexual, envolvendo, ou não, fotografias ou vídeos de nudez das partes envolvidas. Por fim, o *revenge porn* se consiste na conduta de espalhar fotos ou vídeos de nudez da pessoa que lhe enviou (tendo depositado confiança nesta), como uma forma de vingança. Como cita (RODRIGUES, s/d, online), cada termo tem seu significado único:

> Hater: Palavra que significa aquele que odeia. São pessoas que disseminam o ódio no ambiente virtual, atacam outras pessoas com ofensas e humilhações, de forma sistemática.
>
> Sexting: Palavra originada a aprtir das palavras sex (sexo) e texting (ato de trocar mensagem de texto ou conversar por plataformas virtuais). O sexting consiste na troca de mensagens de cunho sexual podendo ou não conter imagens de nudez das pessoas envolvidas. Quando há essa troca de imagens, o sexting pode tornar-se perigoso, pois pode ser divulgado por aquele que recebeu as imagens, ou hackers podem invadir os aparelhos e divulgarem o conteúdo. A divulgação das imagens, que rapidamente viralizam na rede, pode levar a vítima a sofrer com cyberbullying.
>
> Revenge Porn: essa expressão significa, literalmente, vingança pornográfica. Ele diz respeito ao ato de divulgar imagens eróticas e de nudez de uma pessoa que as enviou à outra confiando em sua índole, mas que as divulga como forma de vingança e punição.

Há de se analisar também o fenômeno do *sextortion* (o termo deriva do inglês através da mescla das palavras '*sex*' e '*corruption*') que se caracteriza quando o criminoso obtém conteúdos particulares/privados (fotos ou vídeos de cunho sexual) da vítima, utilizando destes para adquirir alguma vantagem sobre seu alvo. Esses conteúdos podem ser adquiridos através de invasões dos sistemas informáticos da vítima ou, como é mais comum acontecer, de maneira particular através de trocas de mensagens em redes sociais e aplicativos de comunicação.

5. Dados Estatísticos dos Crimes Cibernéticos

Ao passar das décadas, é perceptível a evolução da tecnologia e gradualmente a sua adaptação para o mundo, tendo como tecnologia principal e mais importante da contemporaneidade: a Internet. Muito utilizada principalmente como meio de comunicação, ao acesso às informações (aos aspectos culturais de nações, além das atualizações do momento de cada país), ao mercado (sites de compra virtual) e entretenimento (séries, vídeos, jogos eletrônicos, etc), percebe-se assim as amplas oportunidades de utilização, transformando-a em um grande fenômeno da globalização. Porém é de se perceber que nada dura perfeitamente bem no mundo atual tendo em vista que a Internet também virou meio para a confecção de estratégias no intuito da consumação dos crimes cibernéticos afetando diversos pontos da sociedade, como escrito por Alison Grace Johansen para a *Norton Life Lock*:

> Os ataques cibernéticos são um perigo em evolução para organizações, funcionários e consumidores. Eles podem ser projetados para acessar ou destruir dados confidenciais ou extorquir dinheiro. Com efeito, eles podem destruir empresas e prejudicar suas vidas financeiras e pessoais - especialmente se você é vítima de roubo de identidade. (traduzido).

É de fato axiomático que a Internet proporciona diversas vantagens para as nações observando assim que, além dos inúmeros aspectos positivos, obviamente surgiriam diversos pontos negativos, sendo o principal destes a difícil capacidade para punir os malfeitores ocasionadores dos crimes virtuais. No Brasil, estas características não podiam ser diferentes tendo em vista que se tornou o segundo país no mundo a sofrer casos de crimes cibernéticos (perdendo apenas para a China) dando um prejuízo de aproximadamente 22 bilhões de dólares, segundo dados emitidos em 2017 pela *Norton Security*, onde isso seria resultado por conta da quantidade de usuários de tecnologias, mais especificamente *smartphones*, pois são dois países com um grande quantitativo populacional (UOL, online). Em 2018, a *SaferNet*, em parceria com o Ministério Público Federal (MPF), constatou um total de 133.732 noticiações de crimes cibernéticos no país, tais como pornografia infantil, misoginia, dentre outros (Augusto Fernandes, online). Já em dados emitidos no ano de 2019, através da *SaferNet* Brasil, constata-se que em 2019 houve um aumento de 109,9% dos crimes na internet envolvendo em sua grande maioria crimes voltados contra as mulheres (Fernando Rodrigues, online).

No ano de 2018, segundo o laboratório especializado em crimes virtuais disponível na *Psafe* (dnfdr lab) foram detectados 120,7 milhões de ataques cibernéticos apenas no primeiro

semestre deste mesmo ano (um número bastante destoante com a quantidade de crimes virtuais que resultaram em queixa no mesmo ano de 2018, sendo um abismo de diferença já que foram constatados milhões, onde apenas alguns mil foram levados para a queixa). Nos últimos três meses deste mesmo ano foi constatado um total de aproximadamente 62 milhões de links maliciosos disponibilizados na internet, sendo o meio mais comum o aplicativo de comunicação "*whatsapp*" pois é o mais utilizado no mundo e onde é mais fácil a manipulação de mensagens, onde a maioria destes links estavam voltados para as tentativas de '*phishing*'(resumidamente a vítima ingressa no endereço citado achando que é dotada de conteúdo confiante e seguro quando na verdade é submetido a fisgadas de informações pessoais e até dados de contas bancárias). Segundo o site da Norton, a prática de *phishing* está agredada às fraudes online ou fraudes eletrônicas, que pode essa prática ser conceituada como:

> [...]Os ladrões da Internet atacam usuários sem que eles suspeitem, enviando emails de phishing. Nesses emails, um criminoso cibernético tenta levá-lo a acreditar que está se conectando a um site confiável, no qual você normalmente se conecta. Pode ser um banco, uma conta de mídias sociais, um site de compras online, empresas de envio de remessas, empresas de armazenamento na nuvem e muito mais[...]

5.1 Principais Categorias de Crimes Virtuais ocorridas no ano de 2018

De acordo com os dados apresentados pelo laboratório especializado em crimes virtuais da *PSafe (dfndr lab)*, foram listados quais os crimes que mais ocorreram especificamente no segundo trimestre do ano de 2018 onde, os números são alarmantes pois de acordo com o quantitativo populacional do Brasil, pode-se entender que uma a cada 3 pessoas no Brasil pode ter sofrido por crimes cibernético, segundo Emilio Simoni, o diretor do laboratório:

> Os números são alarmantes, pois, se comparados ao total da população brasileira, segundo dados do Instituto Brasileiro de Geografia e Estatística (IBGE), projeta-se que um em cada três brasileiros pode ter sido vítima de cibercriminosos somente entre os meses de abril, maio e junho de 2018. Somado a isso, nossa análise nos mostra que, a cada segundo, no último trimestre, foram detectados oito links maliciosos. Foram mais de 28 mil detecções por hora.

Os dados apresentam estatísticas a respeito dos crimes de phishing (via aplicativo de mensagem, bancário, de premiação falsa, de e-mail), publicidade suspeita, site com malware, golpe do sms pago, notícias falsas (Fake News), outros:

> *1- Phishing (aplicativo de mensagem): 57,4%*
>
> *2- Publicidade Suspeita: 19,2%*

3- Notícias Falsas: 7%

4- Phishing (de e-mail): 4%

5- Phishing (bancário): 3,8%

6- Golpe do SMS Pago: 3,1%

7- Phishing (premiação falsa): 3%

8- Site com Malware: 1,7%

9- Outros: 0,9%

Os dados relacionados às notícias falsas (comumente conhecidas e disseminadas como Fake News) são dados somados por três tipos de informações: dinheiro fácil, TV e Celebridades (dados únicos) e política. Por fim, dados listados ao relatório expedido pelo laboratório indicam também que diversos hackers se aproveitaram do momento da Copa do Mundo (ainda no ano de 2018) para agirem havendo algum tipo de promessa (na maioria dos casos relacionados à recompensa da camisa da seleção brasileira de futebol).

6 – Legislações e as Fragilidades da Aplicação nos Casos Concretos

A partir da evolução tecnológica mundo afora, vários pontos da sociedade também evoluíram paralelamente, tais como o ramo da saúde e da educação. Não poderia ser diferente com os meios de comunicação e entretenimento onde, ao longo das décadas, desenvolvem-se os meios mais eficazes para tal suprimento, sendo relacionados na grande maioria das vezes à Internet. O seu ambiente cibernético, amplo e vasto de tamanho e proporções descomunais onde é difícil a compreensão de quando as informações tornam-se novas e velhas (por conta da imensidão de informações transmitidas e movimentadas), pode ser utilizado no intuito da realização de diversos desejos, tais como a recepção de aprendizado e compartilhamento de conhecimento, pesquisas, mercado, dentre outros. Percebe-se assim que com o passar dos tempos, na medida em que o número de conexões entre computadores e smartphones cresce de maneira exponencial, também cresce a criminalidade neste meio, onde na maioria das vezes se escondem no anonimato para realização e consumação destes atos delituosos por conta da fragilidade das investigações no meio virtual.

É de se perceber que no Brasil há uma real preocupação e movimentação a cerca de tentar regulamentar e obstruir o prosseguimento dos crimes virtuais por conta da quantidade de

projetos de lei tramitando no Congresso Nacional e algumas leis já vigentes (pode-se citar a lei 12.737/2012 e a lei do Marco Civil da Internet).

Alguns autores e especialistas recomendam a criação de uma legislação que em seu texto preveja as condutas ilícitas possíveis no mundo cibernético, mesmo que já tenha sido tutelado o bem jurídico em questão por outra legislação já vigente, pois essa necessidade se dá pela precariedade de uma norma específica aos crimes cibernéticos. Havendo assim a lacuna a ser suprida referente à legislação, há a divisão dos crimes virtuais em: crimes puros, mistos e comuns, como Arthur Egerwarth cita as palavras de Aurélio (1995) em sua monografia:

> Crimes Puros: "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" (AURÉLIO, 1995);
>
> Crimes Mistos: "Incidiram normas da lei penal comum e normas da lei penal de informática. Da lei comum, por exemplo, pode-se aplicar o artigo 171 do Código Penal combinado com norma de mau uso de equipamento e meio de informática. Por isso não seria um delito comum apenas, incidiria a norma penal de informática, teríamos claramente o concurso de normas" (AURÉLIO, 1995).
>
> Crimes Comuns: "Todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta a perecerão de crime comum, tipificável na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta" (AURÉLIO, 1995).

Entende-se então que, de maneira resumida, os crimes puros são os que utilizam a internet como meio para objetivar danos direcionados ao próprio sistema do computador, intencionados à lesão física ou técnica do APARELHO da vítima (atentados visando a parte física ou ao hardware do aparelho alvo); já os crimes mistos são os que utilizam da internet/computador como meio indispensável (sine qua non) para a consumação do seu crime no intuito de atingir um bem jurídico tutelado da vítima (por exemplo, o artigo 171 do Código Penal versa sobre o estelionato onde fere o patrimônio de quem seja vítima deste tipo de crime, porém deve utilizar da internet/computador como meio para a consumação deste); por último, os crimes cibernético comuns são os que utilizam da informática como ferramenta para consumar o delito que poderia ser realizado também sem a utilização da tecnologia, ou seja, a tecnologia é utilizada para consuma crimes que já são tipificados pela norma penal/Código Penal.

Porém, a discussão a respeito da tentativa de suprir as fragilidades nas investigações e prevenção dos crimes cibernéticos vai mais além do quê a elaboração de legislações intencionadas para tal, onde Emeline Piva Pinheiro em sua monografia acerca dos Crimes Virtuais aborda tal ponderação a respeito de uma política efetiva internacional entre as nações para resultar no melhor treinamento dos agentes investigativos:

> [..] Mas a necessidade urgente é de uma política internacional que dê apoio às polícias mundiais, fornecendo melhores condições e treinamentos para seus agentes, no sentido de tornarem-se capazes de investigar os crimes que ocorrem no ambiente virtual da Internet, além de fomentar a integração entre as nações para assegurar a investigação e coleta de provas destes crimes, por guardarem características peculiares, especialmente se observado sob o prisma da grande possibilidade de ser objeto de execução à distância, envolvendo diversos países e suplantando as fronteiras territoriais em poucos segundos. O treinamento de policiais neste novo ambiente criminoso, assim como adquirir equipamentos capazes de prever e analisar os crimes novos e principalmente a adoção de processos internos para a viabilização de condutas preventivas e de correção são alguns passos essenciais.

O treinamento e qualificação de profissionais e agentes mais voltados ao âmbito virtual poderia ter um efeito maior no combate aos crimes cibernéticos, diminuindo drasticamente os dados relacionados à impunidade dos criminosos por conta do ambiente virtual ser mais volátil e favorável para a consumação de crimes, como prossegue a autora:

> A impunidade dos criminosos virtuais é uma consequência mais da fragilidade das informações de rastreamento do que da falta de legislação específica. Pela natureza da Internet, com seu ciberespaço, é muito difícil fiscalizá-la. O trânsito de dados é livre e veloz, é instantâneo, e como todas esses dados são traduzidos em bits, facilmente manipulados pelos experts, a prova da conduta ilícita é frágil, isso quando resta alguma.

Portanto percebe-se que a fragilidade do combate não está somente na falta de uma legislação específica e própria direcionada aos crimes virtuais, mas também ao 'modus operandi' das autoridades voltados a eles, pois os criminosos estão fazendo uso diverso da tecnologia e conseguindo burlar os modos de operação e investigação das autoridades competentes, devendo assim haver uma movimentação em massa entre as nações, uma cooperação internacional intencionada e voltada para o treinamento e capacitação de agentes (como por exemplo a FBI desenvolvendo os Cybercops) voltados a esses delitos, pois percebe-se que pela vastidão do cyberuniverso, tais delitos serão o novo grande desafio criminal do século.

CONSIDERAÇÕES FINAIS

Analisados os tópicos passados, ficou evidenciado que a tecnologia veio mais para agregar que para retirar, porém a grande necessidade dos seres humanos em expandir as fronteiras tecnológicas deu abertura à negatividade, onde se faz presente destacando-se mais que a positividade evidente. Entende-se que o ciberespaço ampliou o contato entre os povos, bem como aumentou a vulnerabilidade das sociedades aos ataques criminosos no âmbito virtual, destinados à lesão do aparelho tecnológico, às fraudes, às clonagens e qualquer outro meio de obter alguma vantagem ilícita financeira, além dos crimes destinados à ofensa da honra da vítima, tais como calúnia, difamação e injúria (racial e preconceituosa). É de fácil compreensão que as normas atuais não são tão eficazes como propuseram-se a ser direcionadas à punibilidade dos infratores, porém a deficiência real reside nas fracas medidas de investigação e baixo preparo dos agentes direcionados ao ramo cibernético, pois a alta volatilidade do meio virtual é um alto entrave perante as medidas investigativas existentes das autoridades competentes da sociedade contemporânea.

Analisados os pontos citados no artigo fica clara a imensa necessidade de uma movimentação internacional e nacional a fim de tentar compreender as nuances do ciberespaço bem como tentar suprir inúmeras lacunas referentes às investigações e legislações, seja por jurisprudências ou doutrinas, bem como a continuidade de estudos ao passar dos tempos para tentar trazer à tona diversas contribuições, não só ao meio acadêmico como também à sociedade atual.

Por fim, há de se perceber que atitudes como aquelas são de grande necessidade no intuito de conseguir compor uma sociedade digital mais segura e igual, livre das ameaças prejudiciais dos criminosos virtuais que escondem-se no anonimato e prosseguem com seus delitos presos na certeza da falta de punição dos seus atos.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A CRIMINALIDADE INFORMÁTICA**. São Paulo: Editora Juarez de Oliveira, 2006

BOFF, Salete Oro. FORTES, Vinícius Borges. **CRIMES INFORMÁTICOS: POSSIBILIDADES DE CONSTRUÇÃO DE UM MODELO NORMATIVO DE GOVERNANÇA DO CIBERESPAÇO,** 2016.

CARVALHO, https://domtotal.com/direito/pagina/detalhe/29709/crimes-digitais acesso em 20/04/2020

CRESPO, Marcelo Xavier de Freitas. CRIMES DIGITAIS. São Paulo: Saraiva, 2011.

EGEWARTH, Arthur. **OS CRIMES CIBERNÉTICOS E A INEFICÁCIA DA LEI "CAROLINA DIECKMANN"**, 2019

FERNANDES, Augusto - https://www.correiobraziliense.com.br/app/noticia/politica/2019/08/04/interna_politica,775357/crimes-virtuais-e-ataques-ciberneticos-mais-do-que-dobram-em-um-ano.shtml - acessado em 19/05/2020

JOHANSER Alison Grace - https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html - acessado em 19/05/2020

LIMA, Paulo. http://www.cartaforense.com.br/conteudo/entrevistas/crimes-de-computador/8112, acesso em 20/04/2020

LUCCA, Newton. FERREIRA, Ivete Senise A CRIMINALIDADE INFORMÁTICA.

LUCCHESIL, Ângela Tereza. HERNANDEZ, Erika Fernanda Tangerino. CRIMES VIRTUAIS: CIBERBULLYING, REVENGE PORN, SEXTORTION, ESTUPRO VIRTUAL.

PINHEIRO, Emelie Piva. CRIMES VIRTUAIS: UMA ANÁLISE DA CRIMINALIDADE INFORMÁTICA E DA RESPOSTA ESTATAL.

RODRIGUES, Fernando - **https://www.poder360.com.br/justica/denuncias-de-crimes-ciberneticos-aumentaram-1099-em-2018-diz-associacao/ - acessado em 19/05/2020**

RODRIGUES, Lucas de Oliveira. **CYBERBULLYING**. Brasil Escola. Disponível em https://brasilescola.uol.com.br/sociologia/cyberbullying.htm acesso em 30 de Abril de 2020

SCHMIDIT , Guilherme - https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos acesso em 27/05/2020

https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm

https://canaltech.com.br/seguranca/numero-de-ataques-ciberneticos-no-brasil-quase-que-dobrou-em-2018-119600/ - acessado em 19/05/2020