PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

CRIMES CIBERNÉTICOS: O LADO OBSCURO DA REDE

ORIENTANDO (ª) - CLÁUDIO VIEIRA GUIMARÃES LIMA

ORIENTADOR (ª) - PROF. MARISVALDO CORTEZ AMADO

GOIÂNIA
2021

CLÁUDIO VIEIRA GUIMARÃES LIMA

CRIMES CIBERNÉTICOS: O LADO OBSCURO DA REDE

Monografia Jurídica apresentado à Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para obtenção do título de bacharel em Direito.

Prof. (ª) Orientador (ª) - Marisvaldo Cortez Amado.

GOIÂNIA
2021

Resumo

Neste trabalho serão abordados os aspectos históricos e conceituais dos crimes cibernéticos, bem como algumas noções gerais de cibercriminalidade e uma breve explanação das atuais leis brasileiras que tratam do tema. Não obstante, o enfoque da presente pesquisa é um estudo mais aprofundado do exercício do direito à liberdade de expressão e a fim de se determinar os limites ao exercício desse direito na internet, bem como as repercussões dos ataques à honra e à imagem de um indivíduo através desse meio de comunicação global. Para apresentar a relevância desta pesquisa, o capítulo dois trará uma análise de trabalhos correlatos ao tema de autores e doutrinadores renomados no meio acadêmico. Por fim, serão apresentadas possíveis soluções à indagação central do trabalho, a qual se refere aos possíveis meios de coibir o exercício arbitrário da liberdade de expressão.

Palavras-Chave: Cibercrimes. Liberdade. Expressão. Discriminação. Internet.

Abstract

In this work, we will discuss the historical and conceptual aspects of cybercrime, as well as some general notions of cybercrime and a brief explanation of the current Brazilian laws treating this topic. However, the focus of this research is a deeper study of the exercise of the right freedom of speech and to determine the limits to this right at the Internet, as well as the repercussions of attacks at the honour and image of a person, through this global communication. To prove the relevance of this research, in chapter two will bring an analysis of works related to the topic write for renowned authors and scholars in the academic world. Finally, will be present possible solutions for the central question of this work, which refers to the possible means to contain the arbitrary exercise of the freedom of speech.

Keywords: Cybercrime. Freedom. Speech. Discrimination. Internet.

SUMÁRIO

1 INTRODUÇÃO

A necessidade de se abordar um tema tão intrínseco, como o de crimes cibernéticos é de extrema importância, não somente para a seara do Direito Penal, mas também para a comunidade como um todo, principalmente na sociedade contemporânea em que vivemos.

Com o surgimento da informática e a propagação de seu uso, a sociedade se viu diante de uma ferramenta inovadora que foi capaz de tomar conta de suas vidas em diversos aspectos. Logo, a utilização constante de computadores e o acesso fácil à essa enorme rede de dados da internet, fez com esta criação se consolidasse em nossa sociedade. A mesma caminhou a “passos largos” em direção a uma geração dependente da informática, substituindo muitos atos da vida comum pelos sistemas informatizados. Devido à simplicidade e a rapidez com que a internet executa determinada função, o ser humano cada vez mais preferiu as ferramentas virtuais a tal ponto que, hoje, se uma pessoa não possui conta de e-mail ou rede social, é considerada de alguma forma “isolada” da sociedade.

Para entender essa evolução, é válido especular de onde surgiu a internet. A palavra significa “rede internacional” - advindo da união dos termos em inglês Inter (internacional) e net (rede) - e surgiu no fim do século XX. Inicialmente, despontou como ferramenta para internalizar as comunicações em casos de guerra e para estudar as relações entre ser humano e máquinas. Porém, o uso dos computadores era limitado a poucos usuários, pois basicamente era utilizado para uso militar e científico. Somente na década de 1990 a internet tornou-se uma ferramenta pública e de uso indispensável para a sociedade. Concomitantemente com a evolução tecnológica, e devido à sociedade substituir seus atos físicos pelos atos virtuais, surgiu o problema da criminalidade virtual. De acordo com Gustavo Têsta Correa, “A internet é um paraíso de informações, e, pelo fato de essas serem riqueza, inevitavelmente atraem o crime. Onde há riqueza, há crime." A internet é um mecanismo tão recente

e que modificou tão drasticamente a vida do ser humano que pode-se dizer que a humanidade ainda não se adaptou à maneira de viver do século XXI. Em uma era informatizada, o Direito não acompanha a realidade fática da sociedade, principalmente tratando-se de regulamentar as condutas humanas.

A partir de 1980 começou a propagação de diferentes tipos de crimes ocorridos virtualmente, tais como pirataria, transmissão de vírus, pedofilia, invasão de sistemas, entre outros. Conforme tais práticas foram tornando-se expressivas surgiu a necessidade de cuidados com a segurança virtual e, consequentemente, a interferência do Estado para regulamentar tais condutas.

O maior estímulo aos criminosos para o cometimento de crimes na internet é a crença de que lá estão mais protegidos. Isso acontece porque na própria sociedade não existe essa cultura de prevenção de possíveis ataques de criminosos. Talvez por ser um problema relativamente novo na sociedade não se imagina que, ao proteger os computadores e dispositivos, as condutas ilegais serão inibidas.

Logo, essa invenção não trouxe somente benefícios, como a facilidade de integração e a comunicação entre seus usuários, mas também meios para que leis fossem transgredidas e princípios morais e éticos afetados.

O Direito como uma ciência de natureza social, que estuda os fatos juridicamente relevantes para a sociedade, deve acompanhar e se adaptar às inovações, não somente tecnológicas, como é o caso em questão, mas como um todo, buscando assim trazer soluções para os novos problemas que virão a surgir em decorrência dessa modernidade.

Portanto, é diante dessa realidade que o estudo do tema abordado se torna mais relevante, buscando assim entender o que são os crimes virtuais e suas características, auxiliando na aplicação direta do Direito como regulador e organizador da sociedade, empenhando-se na tipificação de tais condutas criminosas que transgridam a ordem legal estabelecida pelo Estado.

2. ASPECTOS HISTÓRICOS E CONCEITUAIS DOS CRIMES CIBERNÉTICOS

A sociedade humana foi se desenvolvendo e passando por transformações e revoluções, e, dentre elas, algumas se destacam. É o caso, por exemplo, da Revolução Francesa, que trouxe o início da positivação de Direitos Fundamentais, sendo tida como fundadora dos direitos civis. A Revolução Industrial, trouxe a substituição das ferramentas pelas máquinas e consolidou o modelo capitalista de produção. Entretanto, os avanços trazidos pelas revoluções sempre acompanham problemas e sacrifícios. Nos casos citados, a Revolução Francesa trouxe morte e sangue, enquanto a Revolução Industrial desemprego e exploração da classe trabalhadora (SYDOW, 2014).

No período mais recente da nossa história, passamos por uma grande revolução, a Revolução Digital, entendida como “o movimento de inserção na sociedade de novas tecnologias e serviços que utilizam desenvolvimentos recentes e que modificam a forma como o cotidiano cidadão progride” (SYDOW, 2014).

Desde a criação da internet, uma das maiores discussões é a respeito da necessidade ou não de regulamentação desse ambiente que surgiu, a princípio, sem nenhum controle impositivo (PINHEIRO, 2014).

Conforme a tecnologia vai fazendo parte do cotidiano humano torna-se fundamental que o indivíduo passe a ter certo conhecimento pressuposto para poder lidar com as modernidades. A informática passou a ser ramo independente de estudo tecnológico, exclusivo e imprescindível para o cidadão que, inclusive, dedica-se a cursos para aprender e melhorar as técnicas utilizadas na rede (SYDOW, 2014).

A partir do momento que a criminologia percebeu que a internet se tornou um novo foco de criminalidade, foi necessária a criação de teorias para definir os crimes virtuais, bem como entender por qual razão eles ocorrem.

Os crimes virtuais, além das características das infrações penais “reais” são identificados como cometidos através do uso de dispositivos tecnológicos. A Organização para Cooperação Econômica e Desenvolvimento da Organização das Nações Unidas (OCDE), em 1983, definiu como crime informático “qualquer conduta ilegal, não ética, ou não autorizada que envolva processamento automático de dados e/ou a transmissão de dados” (PALAZZI, 2000).

Pode-se dividir os crimes virtuais como próprios ou impróprios. Os primeiros, são aquelas condutas antijurídicas e culpáveis que visam atingir um sistema informático ou seus dados violando sua confiabilidade, sua integridade e/ou sua disponibilidade, um exemplo comum são os Hackers. Já os segundos, são condutas comuns – típicas, antijurídicas e culpáveis – que são perpetradas utilizando-se de mecanismos informáticos como ferramenta, mas que poderiam ter sido praticadas por outros meios, como exemplo disso temos o chamado “*Hate Speech”* ou “Discurso de ódio”.

Para que haja participação efetiva e inserção da pessoa no chamado ciberespaço, é necessário que o Estado promova a proteção de seus direitos e garantias fundamentais, não podendo as novas tecnologias servirem de meios para violação desses direitos.

3. A INTERNET E A RELAÇÃO COM O DIREITO

O Direito como ciência social deve acompanhar a evolução do ser humano e da sociedade na qual ele está incluído, atendendo as necessidades de normas que regulamentam as condutas das relações humanas.

Com o surgimento da internet e a disseminação da cultura da globalização, a sociedade caminhou a “passos largos” em direção a uma geração dependente da informática, substituindo muitos atos da vida comum pelos sistemas informatizados. Devido à simplicidade e a rapidez com que a internet executa determinada função, o ser humano cada vez mais preferiu as ferramentas virtuais a tal ponto que, hoje, se uma pessoa não possui conta de e-mail ou rede social, é considerada de alguma forma “isolada” da sociedade.

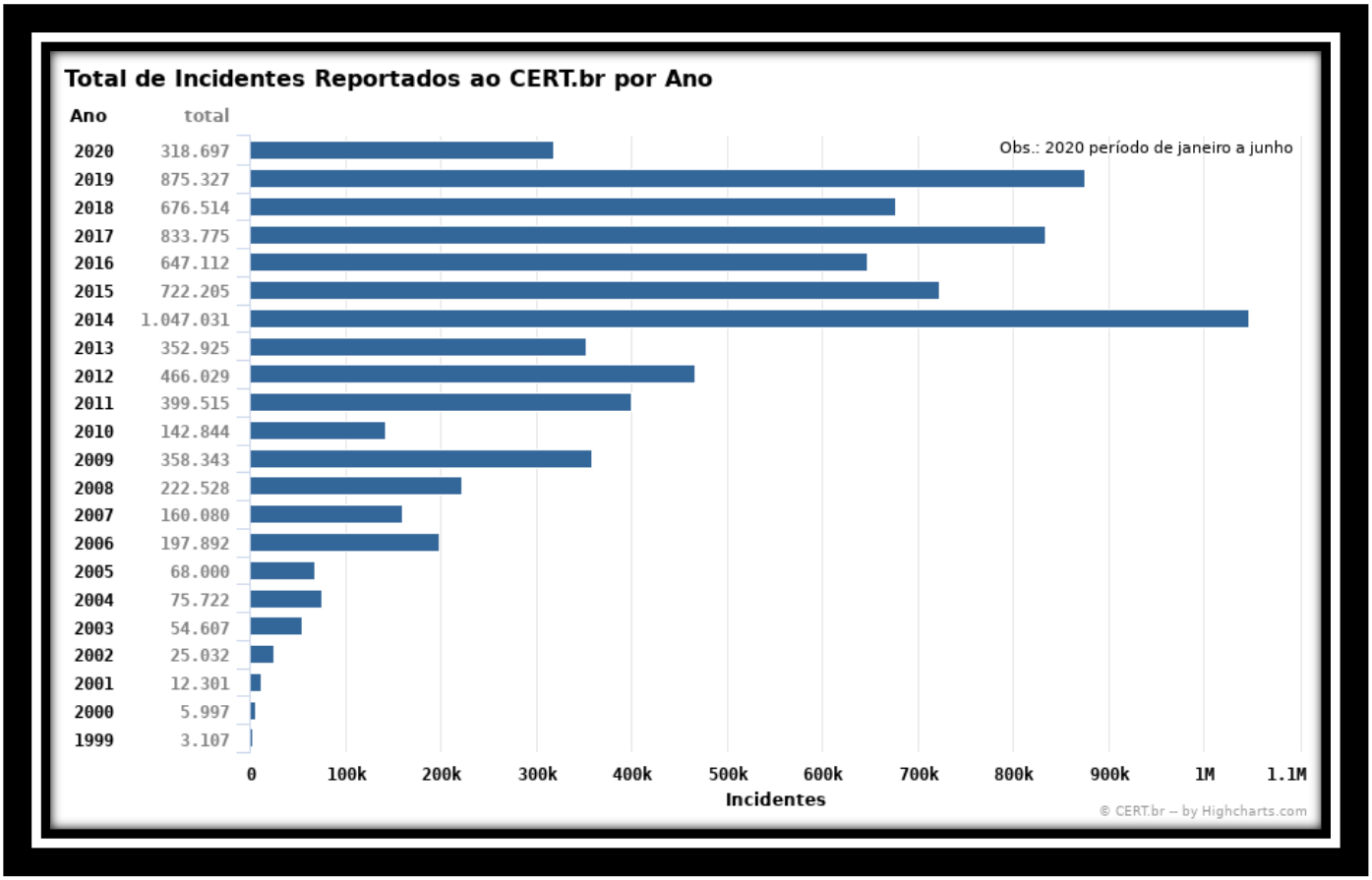
O maior estímulo aos criminosos para o cometimento de crimes na internet é sentimento de impunidade, acreditando assim que lá estão protegidos de certa forma. Isso acontece porque na própria sociedade não existe essa cultura de prevenção de possíveis ataques de criminosos. Talvez por ser um problema relativamente novo na sociedade não se imagina que, ao proteger os computadores e dispositivos, as condutas ilegais serão inibidas.

O Brasil começou a preocupar-se com tais questões recentemente. A promulgação da Constituição em 1988 estabeleceu que as questões de informática deveriam ser de competência do Estado.

Desde a década de 1970 existe menção à figura do hacker no âmbito criminal, à medida que a Internet foi se popularizando. Faz parte do entendimento a respeito do tema compreender de que forma surgiram os crimes virtuais. Uma vez que a Internet se tornou alvo do interesse público, pode-se esperar que nela desenvolvam-se condutas criminosas, visto que o ser humano tende a criar meios ilícitos para todas as atividades do seu dia a dia. Dessa forma, depara-se com a figura do sujeito que pratica tais condutas, o qual pode-se chamar de “cyber criminoso”.

4. OS CRIMES VIRTUAIS

Assim como as práticas de crimes comuns se aperfeiçoam com o tempo, os crimes virtuais também tomam novas formas através do avanço tecnológico que permite e facilita suas práticas. Com o grande número de usuários na internet - que ultrapassou a marca de 4,66 bilhões -, é cada vez mais difícil identificar os agentes que cometem crimes na internet.



Disponível em: https://www.cert.br/stats/incidentes/. Acesso em 15 de março de 2021.

A definição de crimes virtuais é algo recente comparado aos conceitos de crimes tradicionais estudados há muito tempo. Um dos mais conhecidos é o de Krone (2005), que define crimes virtuais como delitos que vão desde atividades criminosas contra dados até as infrações de conteúdo e copyright. Porém, a definição é mais ampla, e inclui atividades como a fraude, o acesso não autorizado, a pornografia infantil e o

assédio na internet. Este trata-se de um crime de meio, ou seja, um crime que se utiliza do meio virtual. Moisés Cassanti, em sua obra “Crimes virtuais, vítimas reais”, conceitua crimes virtuais como "toda atividade em que um computador ou uma rede de computadores é utilizada como ferramenta, base de ataque ou como meio de crime".

Pode-se dizer, portanto, que os crimes virtuais são todos aqueles que ocorrem através ou com o auxílio de meios virtuais, sendo utilizados para a prática de atos ilegais, servindo para renovar a execução de antigos delitos ou para criar novos crimes. Os criminosos virtuais utilizam vários métodos distintos para a prática de seus crimes

4.1 OS CIBERCRIMINOSOS

O agente que pratica conduta típica, antijurídica e culpável constitui os elementos de crime, e será processado, julgado e punido por suas condutas. O mesmo ocorre com o sujeito que pratica tal ato virtualmente.

Para muitos, o *cibercriminoso*, como sujeito ativo, é estereotipado como um jovem, visto que a internet é algo considerado relativamente recente. Já outros passaram a ver qualquer pessoa que possua conhecimento informático, capaz de acessar um computador ou dispositivo, como um criminoso em potencial.

Os agentes responsáveis pelas práticas dos crimes virtuais podem ser tanto pessoas possuidoras de um conhecimento técnico mais profundo a respeito da internet - hackers ou crackers -, quanto usuários comuns que, através de suas condutas virtuais, cometem crimes contra outros usuários. Portanto, não se pode traçar um perfil estigmatizado sobre o *cibercriminoso*.

4.1.1 *Hackers X Crackers*

Quando pensamos em *cibercriminosos,* logo associamos àquelas pessoas que possuem conhecimento técnico e especializado a respeito da internet e dos métodos de se obter informações por meios escusos, consequentemente relacionamos à figura dos chamados *Hackers.* Contudo, na visão de especialistas da área, estes na verdade não constituem os verdadeiros criminosos da internet. Esses seriam denominados *Crackers,* - do termo em inglês *"to crack"*, que significa para quebrar - ou seja, pessoas que utilizam de seu conhecimento informático para quebrar sistemas de segurança e roubar dados e senhas de acesso, bem como invadir redes de forma ilícita para fins criminosos.

Portanto, o termo *Hacker* serve para definir um programador de sistemas, que não necessariamente tem por objetivo causar danos a outrem. Muito pelo contrário, o hacker de hoje é utilizado inclusive para investigar delitos virtuais e colaborar nas investigações e nos desenvolvimentos de softwares de segurança. Assim, podemos entender que *Hacker* é apenas o gênero do qual o *Cracker* é espécie.

4.2 CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Há muitas classificações doutrinárias que definem os cibercrimes. Damásio de Jesus, por exemplo, separa os crimes virtuais em quatro categorias: próprios, impróprios, mistos e mediatos. Para ele, crimes virtuais próprios são aqueles em que o sujeito utiliza necessariamente da ferramenta eletrônica para a prática do delito. Ou seja, são crimes que não podem se consumar sem o computador, uma vez que este caracteriza elemento intrínseco à prática do crime. São exemplos de crimes virtuais próprios: ataque de vírus e *malware.* Damásio ainda complementa: "Neles (crimes virtuais próprios), a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado".

Já os crimes virtuais impróprios são aqueles praticados com o auxílio do computador, quando este é utilizado para executar condutas já tipificadas no ordenamento jurídico como ilícitas. Isto é, a internet é usada como nova ferramenta para a prática de “velhos crimes”, como a pedofilia e o tráfico de órgãos.

Os crimes virtuais mistos são aqueles complexos em que a legislação protege mais de um bem jurídico, ou seja, protege o bem jurídico informático e outro bem jurídico distinto. E por fim, os crimes virtuais mediatos tratam dos delitos praticados com o intuito de alcançar outro fim, que será consumado no mundo real. O exemplo citado por Damásio é do agente que utiliza do crime virtual para capturar dados da vítima e usa-os para desfalcar a conta corrente dela. Considerados estes aspectos sobre a classificação, denota-se de relevante importância fazer breves considerações sobre como tais crimes ocorrem no meio virtual, e quais as formas mais comuns.

4.3 COMO OCORREM OS CRIMES CIBERNÉTICOS

A prática de crimes de Internet é explorada através de vulnerabilidades de segurança nos equipamentos, softwares ou até mesmo pela ingenuidade humana. Antigamente, todas as ameaças eram tratadas como vírus de computador, porém hoje há uma gama imensa de tipos de ataques cujos principais serão explicados a seguir.

4.3.1 PHISHING

O termo é originado do verbo inglês *to fish* que significa pescar e caracteriza a conduta de pesca de informações de usuários. Inicialmente, a palavra *phishing* era usada para definir a fraude de envio de e-mail não solicitado pela vítima, que era estimulada a acessar sites fraudulentos. Uma de suas características é que as mensagens estimulam ser de pessoas ou instituições legítimas como bancos, órgãos governamentais ou empresas. Hoje, a palavra também é utilizada para definir a conduta de pessoas que encaminham mensagens com a finalidade de induzir vítimas a enviar informações para os criminosos.

A técnica de *phishing* já é bem conhecida e a sua conscientização é promovida por grandes provedores de e-mail como Google e Yahoo. As principais ações envolvendo *phishing*, utilizadas pelos atacantes, são mensagens com links para programas maliciosos, ofertas de grandes lucros, fotos de celebridades, notícias sobre tragédias, reality shows, orçamentos e cotações de preço, informações de cobrança em sites de comércio eletrônico, telefonia e provedores de acesso à internet, informações sobre inclusão do seu nome no SPC e Serasa, avisos de órgãos do governo e instalação de módulos de segurança para a realização de transações bancárias.

4.3.2 RANSOMWARE

O *ransomware* é um dos malwares mais temidos pelos usuários, pela maneira que afeta suas vítimas. Em suas primeiras ocorrências, esse malware bloqueava a tela do computador deixando exposta uma mensagem exigindo pagamento para que o computador fosse liberado.

Com o seu sucesso, surgiram diversas novas variantes e, consequentemente, mais perigosas. As novas versões são capazes de criptografar os arquivos do seu dispositivo exibindo informações de como proceder para receber a chave de desbloqueio. O pagamento geralmente é solicitado através de *Bitcoins*, uma moeda eletrônica independente de qualquer autoridade central. É bom lembrar que o pagamento não garante que seus arquivos sejam desbloqueados, afinal como dificilmente é possível identificar o criminoso, também não há como cobrá-lo.

O método mais comum de infecção é através de e-mails de *phishing*, onde o usuário é atraído a clicar em links que direcionam ao download do *ransomware*. Atualmente, também é comum o ataque através de sites populares que foram invadidos e tiveram seus códigos fonte e links alterados.

4.3.3 PORNOGRAFIA INFANTIL

A pornografia infantil talvez seja o crime que mais provoque a repulsa da sociedade. Não há qualquer forma de se aceitar as situações constrangedores a que crianças são subordinadas, para saciar as fantasias de pessoas desequilibradas. A pedofilia é um fenômeno fora dos padrões comuns toleráveis pela sociedade, encontrando na Internet um veículo para satisfazer virtualmente os seguidores dessa prática. Esta modalidade aparece na Internet de duas maneiras: pelas "*home pages*" e por correio eletrônico. Na primeira opção, os gerenciadores das páginas que recebem uma quantia dos usuários (através de depósito ou cartão de crédito), que dispõem de um acervo de fotos e vídeos. Na segunda opção, o material é distribuído de um usuário a outro, diretamente.

Evidencia-se, portanto, um transtorno psicológico que leva o indivíduo a ter desejos sexuais por crianças e adolescentes. Tal transtorno é, inclusive, utilizado como fundamentação para não incriminação do indivíduo, pois no caso seria uma doença.

A Pedofilia pela internet acabou se tornando um mercado para muitos, uma vez que é uma atividade que tem um percentual de lucro muito alto. Os pedófilos conseguem fazer uma organização com outros pedófilos espalhados por todo mundo, com a finalidade de espalharem a pedofilia, seja por fotografias seja por filmagens, chegando, inclusive, a exporem seus próprios corpos durante a relação sexual.

Assim, não há dúvidas de apesar que as práticas pedófilas são antigas, hoje em dia tem uma maior expansão devido à internet e consequentemente um maior dano, uma vez que marca negativamente várias crianças e jovens de maneira brutal. Os criminosos, portanto, se adequaram para esse mundo virtual e conseguiram atrair mais vítimas.

Embora a legislação avance para combater esses criminosos, ainda não é fácil identificá-los, haja vista que a maioria tem um intelecto muito bom e consegue, muitas vezes, sair impune ao crime. Contudo, há um avanço no aparelhamento tecnológico dos investigadores para que eles consigam lutar em equidade de armas como os pedófilos, pois estes costumam ter uma intelectualidade bem refinada em tecnologia.

4.3.4 CYBERBULLYING

O cyberbullying é uma derivação do bullying, que consiste em insultos, intimidações, humilhação e violência entre crianças e adolescentes, mas que nesse novo formato é praticado de forma virtual. São utilizadas ferramentas tecnológicas como celulares e câmeras digitais em ambientes como Internet e redes sociais para disseminar tais conteúdos. Diferente do bullying que ocorre de forma presencial, o cyberbullying pode tomar proporções que nem mesmo o agressor imagina, pela rapidez com que esse tipo de conteúdo é espalhado na Internet.

Embora esse seja um problema mundial, é pouco conhecido pelo grande público e muitas vezes subestimado pelos pais por acharem que se trata de uma brincadeira. A justiça vem decidindo que a responsabilidade por esses delitos é dos pais por não terem educado seu filho de forma correta ou não terem acompanhado o que ele faz na Internet.

Um levantamento realizado pelo instituto de pesquisa Ipsos revelou que o Brasil é o segundo no ranking de cyberbullying no mundo. A pesquisa entrevistou mais de 20 mil pessoas em 28 países. No Brasil, 30% dos pais ou responsáveis entrevistados afirmaram ter conhecimento de que os filhos se envolveram ao menos uma vez em casos de cyberbullying.

4.3.5 CRIMES CONTRA A HONRA

A internet deve ser vista como um ambiente democrático, coexistindo as mais diversas formas de pensamento. Dessa maneira, é um local para o debate das diversas formas e pontos de vistas relacionadas a diversos ou determinados assuntos, contudo, cada indivíduo que faz uso da internet deve se responsabilizar por suas opiniões.

As pessoas possuem o direito a liberdade de expressão e opinião, direito este estabelecido no artigo XIX, da Declaração Universal dos Direitos Humanos: “Toda pessoa tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras” (ONU, 1948).

Contudo, é importante que se tenha consciência do que se expressa ou opina, principalmente quando será publicado na internet, ainda mais se a opinião ou expressão for criminosa. Pois, deve ser defeso toda e qualquer prática de crime pela internet, limitando, de certa maneira, a liberdade de expressão. Isso decorre do fato de que os indivíduos possuem o direito a expor seu pensamento, mas se o fizer de maneira preconceituosa ou se debatendo com as leis, estes devem assumir os resultados de seus atos. Dentre os crimes mais comuns praticados na internet está o racismo, vedado pela Lei nº 7.716/89.

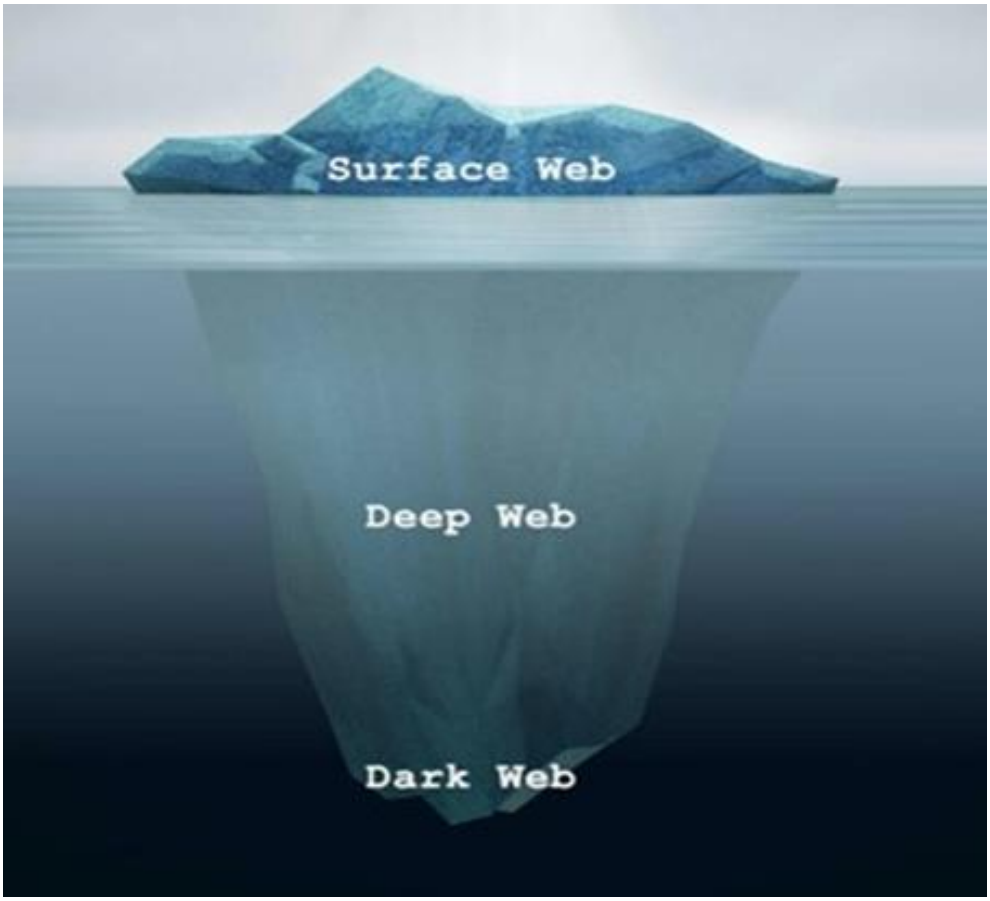
Dessa maneira, do instante que se diz uma palavra ou publica uma imagem/vídeo na internet, estes conteúdos podem afetar diversas pessoas, onde os resultados são independentes da intenção daquele que publicou.

Assim, escrever que não gosta de determinada pessoa é uma coisa, já afirmar que a odeia, associando a pessoa a algum animal, discriminando na internet, proporcionando a ridicularização, acaba por resultar em crime. Os tribunais no Brasil vêm decidindo acerca de diversos casos de ofensas no ambiente virtual, entendendo que a internet é um fator agravador do caso, por ter uma consequência e abrangência maior. Bem como, o Superior Tribunal de Justiça (STJ) vem entendendo quanto os crimes contra a honra praticados em ambiente virtual que a competência é do local onde se encontra o responsável pela divulgação da notícia.

5. A DEEPWEB – O LADO OBSCURO DA INTERNET

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

A Internet convencional, também conhecida como “*Surface Web*”, é formada por computadores com conteúdos conectados entre si, através de uma rede de links espalhados pelo mundo. Na internet comum é possível localizar qualquer máquina desde que se conheça o endereço chamado IP (*Internet Protocol*), ou seja, o IP é um endereço único que cada computador ou servidor possui para ser acessado via Internet.



A *Freenet* ou *Dark Web* possui uma estrutura diferente da *Deep Web* antes retratada, nesse caso, realmente pode ser considerada uma rede “escura”, pois os dados das páginas estão armazenados em um servidor, o endereço TCP/IP e a indexação são dinâmicas, constantemente alteradas e as informações são protegidas por criptografia, onde nem mesmo o servidor que aloca as páginas é capaz de rastrear o conteúdo ou a origem do usuário. Não é difícil em uma pesquisa rápida pela internet, encontrar associada à *Dark Web* a palavra Anonimato, nessas circunstancias estruturais, esse “espaço virtual” ou “ciberespaço” diferente da surface, onde cada “bit” de informação é monitorado ou facilmente rastreado, atualmente com que se dispõe de tecnologia é extremamente improvável que as ações cometidas e compartilhadas na *Dark Web* tenham sua autoria descoberta, tal circunstancia pode ser o vetor para usuários desviantes encontrarem um meio seguro para se organizar e interagir sem consequências jurídicas.

Com isso, os criminosos oferecem desde serviços conhecidos, mas que visam anonimato, como e-mails e redes sociais, até venda de armas, drogas, pornografia, cartões clonados, minérios, e um vasto comércio de crimes digitais.

Neste contexto, verifica-se que o combate à criminalidade na Internet encontra diversos problemas relacionados não somente às lacunas jurídicas, mas também aos reflexos que podem causar na restrição à liberdade de expressão e ao acelerado desenvolvimento tecnológico. O anonimato permitido pela estrutura virtual, que caracteriza a *Deep Web*, dificulta a identificação do autor. Outrossim, a identificação e a localização do criminoso são insuficientes para a lavratura do auto de prisão em flagrante do mesmo, haja vista que tais dados são obtidos, geralmente, quando já transcorrido lapso temporal suficiente para não configurar a prisão em flagrante. Cria-se assim, um sentimento de impunidade nos ciber criminosos que utilizam desses recursos para a prática de seus crimes.

6. INVESTIGAÇÃO POLICIAL A SER APLICADA

Conforme determina a lei 12.735/12 os órgãos da polícia judiciária devem criar setores especializados no combate a crimes virtuais. Somente, alguns estados brasileiros já possuem tais setores, que tem uma delegacia especializada para verificar a ocorrência desses delitos.

Essas delegacias são criadas para verificar a ocorrência dos crimes virtuais na sua especialidade que antes do surgimento da legislação específica não havia delegacias ou órgão especializados nessa área.

O trabalho da polícia judiciária na investigação dos crimes de informática obedece ao mesmo rito de qualquer outro crime, previsto no código de processo penal (Decreto-Lei 3.689, de 3 out. 1941), sendo precedido do registro de um boletim de ocorrência e instauração do inquérito policial. A respeito do inquérito policial, tratam o artigo quarto e seguintes do referido dispositivo legal, prevendo, entre outros detalhes, que a autoridade policial (Delegado de Polícia) procederá a instauração do inquérito policial, logo que tomar conhecimento do fato delituoso, e promoverá todas as ações para buscar a apuração dos fatos e sua autoria, inclusive requisitando perícias técnicas se for o caso.

Nesse sentido, é através do endereço do IP que se verifica o titular da conexão da internet. O IP é um número atribuído pelos provedores de internet sempre que se efetua a conexão é gerado um número diferente de IP, possibilitando assim a identificação do responsável. Portanto, não se pode verificar endereço de IP utilizado em dois computadores ao mesmo tempo.

Devido a crescente criminalidade eletrônica foi criada uma organização não governamental chamada Safernet em parceria com o Ministério Público Federal. Essa organização foi criada para serem denunciados os crimes cibernéticos. São recebidas, encaminhadas e acompanhadas as denúncias on-line sobre qualquer crime ou violação dos direitos humanos praticados através da internet.

Contudo o Safernet é uma associação civil de direito privado que tem atuação nacional, sem fins lucrativos que tem a finalidade de realizar trabalhos baseado em Software Livre, que permite ao internauta acompanhar, em tempo real, cada passo do andamento da denúncia realizada por meio da Central Nacional de Denúncias que do total de denunciantes, 99% escolhem a opção de realizar a denúncia anonimamente. E ao 1% restante é garantido total e completo anonimato.

O Safernet recebe a denúncia, analisa o conteúdo, comprovando a sua materialidade e encaminha ao Ministério Público e a Polícia Federal para que possam descobrir quem praticou tal delito e assim aplicar a devida punição ao criminoso.

7. LEGISLAÇÃO INTERNACIONAL ACERCA DO ASSUNTO

No âmbito internacional, a convenção de Budapeste é a referência para se tratar de crimes virtuais. A Convenção sobre o Cibercrime, aprovada pelo Conselho da Europa em 2001, é considerada um parâmetro legislativo mundial a respeito dos crimes na internet, sua tipificação e persecução. A convenção já foi assinada por 43 países, tendo sido ratificada por 21 das nações signatárias – grupo que inclui países da União Europeia (como França, Itália, Portugal e Espanha) e Estados Unidos, Canadá, Japão, África do Sul, Austrália, Chile e Argentina, por exemplo. O Brasil só foi convidado a aderir ao acordo no ano passado, após anos de trabalhos coordenados pelo Ministério Público Federal junto a órgãos governamentais e inciativa privada.

O objetivo é facilitar a cooperação internacional para o combate ao crime cibernético. A convenção prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional.

A Convenção recomenda, ademais, que as partes signatárias adotem medidas legislativas para tipificar crimes cibernéticos, tais como infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos, infrações relacionadas com computadores, infrações relacionadas com conteúdo e infrações relacionadas com a violação do direito de autor e direitos conexos.

A adesão dos países à Convenção gera segurança jurídica, para que assim todos possam trabalhar juntos no combate aos crimes cibernéticos. Com isso, é necessário transparência, evitando abusos, como a entrega irregular de dados ou atos autoritários dos entes estatais.

8. CONCLUSÃO

Diante dos avanços tecnológicos vistos diariamente, um dos que mais proporcionou novos recursos e funcionalidades foi, sem dúvida, a Internet. Contudo, a mesma evolução que traz benefícios também abre portas para que pessoas mal-intencionadas usem esses recursos para enganarem pessoas, roubarem informações e dinheiro, causando danos a cidadãos de bem.

Entendendo que o tema abordado é de extrema relevância para a legislação brasileira, uma vez que a globalização e a inserção da tecnologia estão totalmente presentes no meio profissional e pessoal das pessoas.

Compreendendo que já existem leis previstas tratando e amparando crimes cometidos pelo meio virtual, porém a fragilidade dessas mesmas leis não pode se manter tendo em vista a grande demanda de processos que clamam um posicionamento eficaz para suas tipificações. A temática precisa ser evidenciada e tratada de forma emergente considerando os projetos de lei, tendo em vista que este é o caminho para que tais projetos se tornem definitivamente leis promulgadas e publicadas para amparar a sociedade como todo.

9. REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL, Lei geral de proteção de dados pessoais. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. Rio de Janeiro: Brasport, 2014.

CORRÊA, Gustavo Testa. Aspectos jurídicos da internet. Saraiva, 2008.

DA PAIXÃO BATISTA, Soily Braga; EUFRÁSIO, Emília. A INVIOLABILIDADE DO DIREITO A PRIVACIDADE NO ÂMBITO DA INTERNET. PROJEÇÃO, DIREITO E SOCIEDADE, v. 7, n. 2, p. 87-98, 2016.

DORNELAS, Natália Alves. A RESPOSTA ESTATAL QUANTO AOS CRIMES CIBERNÉTICOS: UMA ANÁLISE DIRECIONADA ÀS LEIS Nº 12.735/2012 E 12.737/2012.

D'URSO, Luiz Augusto Filizzola. Cibercrime: perigo na internet. Publicado em 2017. Disponível em <http://politica.estadao.com.br/blogs/faustomacedo/cibercrime-perigo-na-internet/>.

HUMANOS, DECLARAÇÃO UNIVERSAL DOS DIREITOS. Declaração universal dos direitos humanos.

JESUS, Damasio de; MILAGRE, José Antonio. Manual de Crimes Informáticos. São Paulo: Saraiva, 2016.

MAZONI, Ana Carolina. Crimes na Internet e a Convenção de Budapeste. 2009.

MENDES, Maria Eugenia Gonçalves; VIEIRA. Natália Borges. Os crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica. Disponível em: http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2

MOREIRA, Antonio Eudes Nunes. A internet e a globalização. Disponível em: < https://www.melodiaweb.com/373/tecnologia/a-internet-e-a-globalizacao>.

MUNIZ, Ronaldo Pereira. Crimes decorrentes de preconceito-lei nº 7.716/89 análise dos princípios e dos mandados de criminalização. Intertemas ISSN 1516-8158, v. 12, n. 10, 2007.

PAESANI, Liliana Minardi. Direito e Internet: liberdade de informação, privacidade e responsabilidade civil. 1ª ed. São Paulo, Atlas: 2000.

PALAZZI, 2000, apud FIORILLO; CONTE, 2016, p. 186

PINHEIRO, Patricia Peck. Direito Digital. 8. ed. rev. atual. e ampl. São Paulo: Saraiva, 2010.

SANTOMAURO, Beatriz. Cyberbulling: a violência virtual. Publicado em 2010. Disponível em <https://novaescola.org.br/conteudo/1530/cyberbullying-aviolencia-virtual>.

SAWAYA, Márcia Regina. Dicionário de informática e internet. São Paulo: Nobel, 1999.

SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallaz Tomaz. Relações Jurídicas Virtuais: Análise de Crimes Cometidos com o Uso da Internet. Revista Cesumar Ciências Humanas e Sociais Aplicadas, v.21, n.1, p. 7-28, jan./jun. 2016.

SOUSA, Lindenberg Barros. Redes de computadores: guia total. 1. ed. São Paulo: Érica, 2009.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as leis brasileiras. Seminário Cibercrime e Cooperação Penal Internacional, n. 1, 2009.

SYDOW, Spencer Toth. Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática. 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/delitos_informaticos_proprios_uma_

abordagem_sob_a_perspectiva_vitimodogmatica.pdf>. Acesso em: 20 nov. 2020.
_____. Delitos informáticos e suas vítimas. 2. ed. São Paulo: Saraiva, 2014.