

Data de aprovação: ____/____/____

CRIMES CIBERNÉTICOS: AVANÇOS DOS “CIBERCRIMES” E UMA ANÁLISE DA LEGISLAÇÃO E DIFICULDADE DE O COMBATE NO BRASIL

Matheus Felipe Miguel Pereira¹

João Batista Machado Barbosa²

RESUMO

Com o avanço e desenvolvimento dos meios virtuais e a Internet, o presente trabalho visa explicar sobre os crimes cibernéticos, abordando os aspectos históricos e conceituais, partindo de uma breve explanação sobre o surgimento desses crimes no ambiente virtual e uma análise da atual legislação pétrea que trata sobre o tema. Será realizado um estudo comparativo entre a legislação internacional e o nosso ordenamento jurídico, com destaque nas leis mais atuais como a Lei Carolina Dickmann e a Lei Marco Civil da Internet. Por fim, serão apresentadas possíveis soluções à indagação central do trabalho, quais seriam os possíveis meios de coibir essas condutas de forma eficaz. Trata-se de um tema atual e com grande relevância para o Direito Penal.

Palavras-chave: Crimes Cibernéticos. Direito Penal. Internet. Tecnologia. Globalização.

CYBER CRIMES: PROGRESS OF "CYBER CRIMES" AND ANALYSIS OF THE LEGISLATION AND DIFFICULTY OF COMBAT IN BRAZIL

ABSTRACT

With the advance and development of the virtual environments and the Internet this act intends to explain cyber crimes, approaching the historical and

¹ Acadêmico do Curso de Direito do Centro Universitário do Rio Grande do Norte (UNI-RN). E-mail: mathmpe@gmail.com

² Professor Orientador do Curso de Direito do Centro Universitário do Rio Grande do Norte (UNI-RN). E-mail: jbmb@uol.com.br

conceptual aspects, starting with a brief explanation about the emergence of these crimes in the virtual environment and an analysis of the current legislation that treats about the theme. A comparative study will be carried out between the international legislation and our legal system, with emphasis on the most current laws such as the Carolina Dickmann Law and the Civil Law of the Internet. Finally, possible solutions will be presented to the central inquiry of the work, what would be the possible ways to effectively restrain these behaviors. This is a current topic with great relevance for Criminal Law.

Keywords: Cyber Crimes. Criminal Law. Internet. Technology. Globalization.

1 INTRODUÇÃO

O Direito está diretamente ligado com a evolução da sociedade e, conforme o seu desenvolvimento, todo o ordenamento jurídico deve também passar pelo processo mutatório para se adequar aos seus anseios. Com o advento da internet e a facilidade de utilizar essa rede em quase todos os lugares, houve o surgimento de novos meios de interações sociais e com isso, passamos a identificar, no meio virtual, a prática de crimes já tipificados no nosso Código Penal.

Hoje em dia, encontramos constantemente práticas abusivas através das redes sociais, especialmente os crimes que atentam contra a honra (injúria racial, calúnia e difamação) e a criação e disseminação de notícias falsas, as chamadas “fake news”, havendo uma linha muito tênue entre a liberdade de expressão e a imposição de censura por parte do estado.

Além disso, outras modalidades de crimes foram surgindo nesse meio e, apesar do constante avanço tecnológico e da realidade desses delitos em nosso país, ainda encontramos dificuldade para identificação dos autores e punição dos mesmos.

Para completar esse cenário, enfrentamos uma situação ainda mais inquietante no Brasil, devido à ausência do legislador quando se fala de privacidade na Internet e aos inúmeros sites que não se comprometem com a adoção efetiva de regras de privacidade. Diante disto, a sociedade indaga como o Estado deve controlar e coagir as mencionadas condutas.

Em busca de responder tal questionamento, o presente artigo,

preliminarmente, busca esclarecer sobre a criação e evolução histórica do computador e da Internet. Posteriormente, conceitua-se o que vem a ser crimes cibernéticos analisando alguns casos concretos e as leis vigentes. Após, foi realizando um estudo comparativo com a legislação dos Estados Unidos, Portugal e ainda foi exposto sobre a Convenção de Budapeste. Por fim, serão apresentadas possíveis soluções à indagação central do trabalho, quais seriam os possíveis meios de coibir essas condutas de forma eficaz

O método de abordagem utilizado nesse projeto foi o método dialético, pois, a pesquisa parte da análise real do que acontece hoje no Brasil, levando em consideração todo um contexto macro para responder e analisar a solução de um assunto particularizado.

Os métodos de procedimento escolhidos no projeto foram os estatísticos, pois pretende trabalhar com os índices do aumento no número de casos no nosso país, ao passo que busca identificar quais os crimes mais praticados. Além disso, a metodologia de estudo de caso também foi aplicada no presente trabalho, pois pretende analisar os casos e como eles ocorrem, para estudar formas mais eficazes de combate. Ademais, foi usado o método comparativo, onde será realizado um paralelo das leis, e projetos de leis existentes em legislações internacionais.

Diante disso, com relação as técnicas de pesquisa empregadas, aplicam-se as leis e projetos de leis, súmulas, doutrina, e casos com repercussão nacional.

2 ASPECTOS HISTÓRICOS

Para entendermos melhor o contexto desses crimes, é necessário abordarmos alguns aspectos históricos do surgimento do computador e evolução da rede mundial de computadores, demonstrando como ela se tornou uma poderosa ferramenta utilizada para boas práticas, como também para o cometimento de atos criminosos.

O primeiro protótipo de computador foi criado ainda nos anos de 1830, por Charle Babbage, cuja intenção era construir um aparelho inteligente, com múltiplos propósitos, capaz de simular o raciocínio humano. Entretanto, devido a inexistência de equipamento adequados e falta de verba, Babbage não conseguiu efetivar a sua invenção. Já durante a Segunda Guerra Mundial, Alan Turing, cujo título de “pai da computação” foi atribuído, durante trabalho desempenhado ao governo britânico, foi

responsável pela criação de uma máquina capaz de quebrar códigos alemães. Pode-se dizer que o dito cientista foi o maior responsável pelo avanço da criptografia como ciência, ao expor a fragilidade dos sistemas época (SCHECHTER, 2016).

Em 1946, mais de 100 anos depois, surgiu o primeiro computador digital eletrônico em larga escala: o *Electrical Numerical Integrator and Calculator*³ (ENIAC), desenvolvido por Konrad Zuse e Jhon Atanasoff e financiado pelo governo dos Estados Unidos. O equipamento pesava cerca de 30 toneladas e ocupada uma área de mais de 140 metros quadrados, composto por válvulas e circuitos eletrônicos. A segunda geração de computadores ocorreu a partir da década de 50, marcada pela substituição das válvulas por transistores, que funcionavam de forma mais rápida e mais confiáveis, além de serem menores fisicamente.

Após a década de 60, entramos na terceira geração dos computadores, que se caracterizou pelo funcionamento a partir de circuitos integrados, possibilitando a construção de vários circuitos de forma simultânea, facilitando assim, a produção em massa. Somente a partir de 1977, ocorre o surgimento da quarta geração, marcada pelo advento de processadores e sistemas operacionais, tornando as máquinas mais confiáveis, rápidas e bem menores do que aqueles das gerações anteriores, o que refletiu na expansão dos computadores pessoais de forma global. Durante esse período, precisamente a partir da década de 90, foram lançados softwares de melhor qualidade e processadores de informações cada vez mais velozes. Com a virada do milênio, houve o desenvolvimento dos chamados computadores de mão, sendo os mais utilizados hoje em dia, como por exemplo os tablets e smartphones, que, além de realizar chamadas, possuíam acesso a rede mundial de computadores, popularmente chamada de internet. Abaixo, podemos perceber a evolução que esses sistemas tiveram, sobretudo, com relação as suas características físicas.

³ Que em português quer dizer Computador e Integrador Numérico Eletrônico

Figura 1 – Evolução dos Computadores

FONTE: DiAna (2017).

O surgimento da internet se deu durante a Guerra Fria, nos anos 60. (EDWARDS, 1996). Durante esse período, os Estados Unidos desenvolveram uma ferramenta capaz de percorrer vários caminhos para que uma mensagem chegasse a determinado destino, servindo assim, como meio de comunicação do exército norte americano. Chamada de *Advanced Research Projects Agency*⁴ (ARPANET), a primeira rede de internet, estabeleceu a primeira conexão entre a Universidade da Califórnia e o Instituto de Pesquisa de Stanford.

Nos anos seguintes houve uma grande revolução tecnológica. Em 1990 foi lançada a World Wide Web⁵ (www), que possibilitou a transmissão de imagens, vídeos e sons, além dos textos que já era possível através da ARPANET. Foi aí que a internet se popularizou pelo mundo, iniciando a criação de diversos browsers e navegadores, como Internet Explorer, Netscape, Mozilla Firefox, Google Chrome, Opera, Lynx.

De acordo com a definição de Zanellato (2002. p.173), “A Internet é um suporte (ou meio) que permite trocar correspondências, arquivos, ideias, comunicar em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos”.

Diante dessa popularização, a internet deixou de ser um sistema restrito as minorias e passou a ser o meio de comunicação mais utilizado entre as pessoas. Seja em computadores, tablets, ou smartphones, os indivíduos estão cada dia mais conectados, utilizando-se desses aparelhos para diversão, trabalho, estudo, e entretenimento, tornando-se essenciais na vida das pessoas. Segundo relatório produzido pelo IBGE divulgado em 2017, 64,7% da população brasileira possui

⁴ Agência de Pesquisas em Projetos Avançados.

⁵ Rede mundial de computadores.

acesso à internet.

Toda essa transformação e evolução da internet, onde a troca de praticamente totalidade das informações ocorrem de forma criptografadas, passou a chamar a atenção dos criminosos, levando ao surgimento dos crimes cibernéticos, objeto de estudo do próximo capítulo.

3. CRIMES NO AMBIENTE CIBERNÉTICO

3.1 CONCEITO

O termo “cibercrime” surgiu no final da década de 90, durante uma reunião do subgrupo de nações do G8, ocorrida na França. A dita palavra era utilizada para descrever todas as modalidades de crimes praticados na internet, que estava cada vez mais acessível ao redor do mundo. Atualmente, doutrinariamente, esse significado é objeto de amplo estudo.

De acordo com Augusto Rossini (2004, p. 110):

[...] 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, disponibilidade e a confidencialidade.

Já Fabrício Rosa (2002, p.53.) conceitua como sendo:

A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O ‘Crime de Informática’ é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o ‘Crime de Informática’ pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à

integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

Por sua vez, Sérgio Marcos Roque (2007, p. 25) entende que os crimes cibernéticos é “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”.

Não diferente das infrações tradicionais, os crimes cibernéticos seriam aqueles de conduta típica e ilícita, de forma dolosa ou culposa, comissiva ou omissiva, porém, praticados com uso da informática, seja conectado a internet ou não.

Junto com o desenvolvimento e o uso global desse recurso, alguns indivíduos começaram a utilizar conhecimentos técnicos e aprimorados para roubar informações criptografadas. Hoje em dia, existe uma infinidade de lojas virtuais, onde as pessoas são atraídas pela facilidade de realizar suas compras sem sair de casa. Além disso, é possível fazer inúmeras transações bancárias, sem a necessidade de enfrentar filas, utilizando apenas o celular, por exemplo.

A doutrina pátria buscou classificar os crimes cibernéticos em 3 grupos: puros, mistos e comuns. Sobre o tema, aponta Teixeira (2014):

O primeiro são aqueles em que o sujeito visa especialmente o sistema de informática; as ações materializam, por exemplo, por atos de vandalismo contra a integridade do sistema ou pelo acesso desautorizado ao computador. Crime de informática misto se consubstancia nas ações em que o agente visa o bem juridicamente protegido diverso da informática, porém o sistema de informática é ferramenta imprescindível. E os crimes de informática comum são condutas em que agente utiliza o sistema de informática como mera ferramenta, não essencial à consumação do delito.

Assim, podemos observar que o puro seria aquele cujo objetivo é atingir o hardware e/ou software de um computador, tanto a parte física quanto a tecnológica do micro. Normalmente, tais condutas são praticadas por Hackers, indivíduos com um vasto conhecimento informático e que se valem deste para identificar falhas do sistema, utilizando-as como ferramentas para extrapolar os limites de funcionamento “normais” dos sistemas.

Já o misto é caracterizado pela utilização da Internet ou computador para realizar a uma conduta ilícita, embora o objetivo do indivíduo não tenha relação direta com a informática ou softwares. Exemplo: as transações ilegais de valores de

contas correntes.

Por fim, o comum é aquele onde o indivíduo utiliza a Internet apenas como forma de instrumento para realizar crime já enquadrado no Código Penal. Exemplos: Pedofilia, crimes contra a honra, apologia ao crime.

3.2 OS PRINCIPAIS CRIMES CIBERNÉTICOS

Diariamente são praticados os mais diversos tipos de crimes no ambiente virtual. De acordo com o relatório produzido pela empresa Norton Cyber Security, o Brasil é o segundo país no mundo com maior número de crimes cibernéticos, afetando em torno de 62 milhões de pessoas e causando um prejuízo estimado em US\$ 22 bilhões.

Com o advento da informática, não apenas surgiram novos delitos, como também potencializou alguns já tipificados e tidos como tradicionais. Segundo Colares (2002, p. 2):

São exemplos de crimes que podem admitir sua execução no meio cibernético: crime contra a segurança nacional, preconceito, discriminação de raça- cor- etnias, pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software, calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação de direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, incitação ao crime, apologia ao crime ou criminoso, falsa identidade, inserção de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões e jogo de azar.

Conforme exposto anteriormente, alguns destes crimes já possuem legislação específica, mas ainda há a necessidade de mudanças para que se adaptem à sua consumação quando perpetrados na rede mundial de computadores. Na tabela abaixo são expostas as condutas criminosas mais comuns no ambiente virtual, acompanhado de suas respectivas tipificações.

Tabela 1 – Algumas condutas criminosas mais comuns no ambiente virtual

CONDUTA	TIPIFICAÇÃO
Estelionato e furto eletrônicos (fraudes bancárias)	arts. 155, §§ 3º e 4º, II, e 171 do CP
Invasão de dispositivo informático e furto de dados	art. 154- A do CP
Falsificação e supressão de dados	arts. 155, 297, 298, 299, 313-A, 313-B do CP
Cyberbullying (veiculação de ofensas em blogs e comunidades virtuais)	arts. 138, 139, 140 do CP
Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional	art. 20 da Lei nº 7.716/1989
Pornografia de Vingança	Ainda não tipificado
Disseminação de notícias falsas	Ainda não tipificado

Fonte: Elaboração do autor (2018).

A seguir, abordaremos algumas destas condutas, expondo casos de relevância nacional e mostrando como o Direito Penal vem se posicionando frente aos problemas.

3.2.1 Invasão de dispositivo informático

A popularidade de smartphones e computadores trouxe grandes riscos, muitas vezes imperceptíveis para os usuários. De acordo com o Art. 154A do CP., incluído pela Lei 12.737, de 2012, o crime de invasão de dispositivo informático se caracteriza no fato do agente:

Art.154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Assim, para sua caracterização são exigidos alguns elementos: a) o núcleo invadir; b) dispositivo informático alheio; c) conectado ou não à rede de

computadores; d) 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; f) ou instalar vulnerabilidades para obter vantagem ilícita.

No ano de 2012, ocorreu uma situação que virou notícia em todo país. A atriz Carolina Dieckmann teve mais de 30 fotos íntimas publicadas na internet que foram furtadas de seu computador através de seu e-mail. Os criminosos, mediante chantagem por meio de mensagens eletrônicas anônimas, tentaram extorqui-la, solicitando determinada quantia em dinheiro para que as fotos fossem deletadas e não divulgadas no mundo virtual. Entretanto, após investigação promovida pelas autoridades competentes, os invasores foram identificados e localizados, sendo, após o devido processo legal, indiciados pelos crimes de extorsão qualificada, furto e difamação. Sobre o caso, convém destacar que no transcurso das investigações, os criminosos compartilharam o produto do seu crime, expondo a vítima ao constrangimento de ter sua intimidade espalhada por toda a internet.

O citado caso teve repercussão nacional e trouxe ao cenário a discussão sobre a necessidade de uma lei que combatesse esse tipo de conduta. Diante disto, o Congresso Nacional se movimentou e promulgou a Lei 12.737/2012, batizada como Lei Carolina Dieckmann, que prevê sanção penal para tais atos:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Art. 2º O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B: "Invasão de dispositivo informático Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. § 3º Se da invasão resultar a obtenção 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 crime 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 obtidos. § 5º Aumenta-se a pena de um terço à metade se 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 de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.” (Grifo nosso) “Ação penal Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Todavia, podemos observar que o legislativo não se preocupou diretamente com os crimes cibernéticos em espécie, mas sim, com pressão social devido ao caso da atriz e visando também uma proteção maior para os próprios membros dos três poderes, como é perceptível no §5º.

Mesmo diante do produto legislativo supramencionado, que busca reprimir tais condutas nos meios virtuais, recentemente alguns criminosos também extraíram e disponibilizaram dados de usuários da loja virtual da C&A, entre eles: número do cartão, CPF, e-mail, valor adquirido como presente, número do pedido e data da compra. O hacker chamado @j0shua afirmou que estão expondo os dados de quatro milhões de pedidos. Esses ataques por vezes possuem a finalidade de demonstrar a fragilidade dos sistemas utilizados, onde as lojas armazenam dados como endereços de clientes, telefone, cartão de crédito, dentre muitos outros. Até o momento não foi identificado o criminoso e o Ministério Público abriu um procedimento administrativo para apurar as consequências do crime.

3.2.2 Fraudes virtuais

Segundo Lima (2002, p. 53), o conceito de fraudes virtuais é tido como:

Fraudes eletrônicas – invasão de sistemas computadorizados e posterior modificação de dados, com o intuito da obtenção de vantagem sobre bens, físicos ou não, por exemplo, a adulteração de depósitos bancários, aprovações em universidades, resultados de balanços financeiros, pesquisas eleitorais, entre outros.

Ainda em sua obra, o Lima entende que para que seja consumado a fraude virtual, é necessário que haja a invasão, modificação supressão ou pagamento de informações, dados eletrônicos ou outro meio que possa realizar alterações em um sistema de processamento de dados por parte do agente. (Lima, 2002)

Existe uma ligação deste crime com o *phishing*⁶, onde os criminosos utilizam e-mails falsos solicitando atualização de dados, informações, muito com bancos e instituições financeiras onde o usuário já possui um vínculo. Assim, ao clicar no link o indivíduo é direcionado para uma página falsa da instituição e, ao inserir os dados sigilosos, os criminosos captam essas informações, resultando, muitas vezes, em vários prejuízos ao usuário.

O citado mecanismo é uma prática bem comum em lojas online, uma vez que houve um avanço no mercado virtual e essa modalidade de compra passou a ser alvo dos criminosos. Lojas falsas, ofertas falsas, atraem os consumidores ao site e, ao realizarem o cadastro, os criminosos tem acesso aos seus dados e conseguem realizar várias transações em seu nome.

3.2.3 Racismo e injúria racial

Como já mencionado em outros momentos, com o avanço tecnológico, percebemos o surgimento de alguns crimes e novas formas de crimes já tipificados em nosso ordenamento jurídico. Mudam-se a forma, os instrumentos, as maneiras de consumá-los, e aí a necessidade de observar a nossa legislação para que seja mantida a proteção dos direitos individuais trazidas pela nossa Constituição Federal.

É importante destacar a diferença dos crimes de racismo e a injúria racial. Entende-se que o crime de racismo afeta uma coletividade, um grupo. Já a injúria racial é direcionada para alguém individualmente.

Com relação a este delito, recentemente, tivemos um caso de grande repercussão, onde a filha do casal Giovana Ewbank e Bruno Gagliasso foi alvo de ataques preconceituosos pela socialite Day McCarthy, que ofendeu a criança em um vídeo feito em uma de suas redes sociais. Os pais da criança prestaram queixa e foi aberto inquérito para apurar o caso, a conduta se enquadra no art. 140, §3º, do Código Penal, contudo, como a agressora realizou as postagens fora do Brasil, será necessário observar a questão territorial, uma vez que, de acordo com o artigo 6º, do Código Penal Brasileiro, instituído pela Lei nº 7.209/84 considera-se praticado o crime “no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.

⁶ Contemporaneamente, a palavra phishing é utilizada para identificar mensagens eletrônicas que hospedam links fraudulentos.

Em caso semelhante, a apresentadora Maria Júlia, do Jornal Nacional, também sofreu diversos ataques e inúmeras ofensas em virtude da sua cor e cabelo, perpetrada na rede social nominada Facebook.

Diante isto, há uma discussão sobre até onde iria a liberdade de expressão nesse ambiente, mas o Supremo Tribunal Federal já adentrou ao tema, fixando entendimento de que a liberdade de expressão é um direito preferencialmente de elevado valor, contudo, comporta limitações, não podendo abranger discursos de ódio e sendo puníveis condutas de discriminação e preconceito publicamente proferidas, conforme decisões dadas pela corte suprema no HC 82.424.

Portanto, condutas como estas devem ser punidas, mesmo que, algumas vezes, estejam projetadas como divulgação de ideias. Hoje em dia, o ambiente mais propício e fácil para ações como esse é na Internet e muitas vezes o anonimato concedido aos usuários impulsionam a prática de crimes como esses. Fazendo-se presente mais uma vez a dificuldade nas investigações para comprovação da autoria e materialidade do crime, não sendo comprovada, o juiz poderá absolver o réu baseado no Art. 386 do Código de Processo Penal:

Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça: I - Estar provada a inexistência do fato; II - Não haver prova da existência do fato; III - Não constituir o fato infração penal; IV - Estar provado que o réu não concorreu para a infração [...] V - Não existir prova de ter o réu concorrido para a infração penal;

Além disso, algumas empresas se recusam a colaborar com as investigações dificultando o colhimento de provas fundamentais para a materialidade do crime. O WhatsApp, por exemplo, já teve suas atividades bloqueadas devido ao não cumprimento de uma determinação da Justiça. O Ministério Público, a Polícia e o Judiciário encontram bastante dificuldade para punir os agentes deste crime. Carlos Eduardo Sobral, chefe da Unidade de Repressão a Crimes Cibernéticos da Polícia Federal, afirmou na CPI dos crimes cibernéticos que: “O volume de investigação vem crescendo, e o efetivo tem que crescer na mesma proporção. Hoje o nosso efetivo acaba sendo menor do que o volume que necessita para que seja dado um rápido andamento às investigações”.

3.2.4 Pornografia de vingança

A pornografia de vingança é um fenômeno recente resultando da crescente globalização da Internet. A dita conduta em expor de forma não autorizada vídeos ou fotos íntimas na rede mundial de computadores sendo, a maioria das vítimas, mulheres que possuíam algum tipo de relacionamento com o agressor.

Marcelo Crespo (CRESPO, 2015), a pornografia de vingança é fixada como:

Exatamente nesse contexto que temos verificado cada vez mais em nossa sociedade a prática do chamado revenge porn, ou pornografia da vingança, que é uma forma de violência moral (com cunho sexual) que envolve a publicação na internet (principalmente nas redes sociais) e distribuição com o auxílio da tecnologia (especialmente com smartphones), sem consentimento, de fotos e/ou vídeos de conteúdo sexual explícito ou com nudez. As vítimas quase sempre são mulheres e os agressores, quase sempre são ex-amantes, ex-namorados, ex-maridos ou pessoas que, de qualquer forma, tiveram algum relacionamento afetivo com a vítima, ainda que por curto espaço de tempo.

Portanto, verifica-se que a prática desta agressão se deu devido à ausência de legislativa sobre o assunto, projetos de leis que visam criminalizar a conduta. O objetivo do agressor ao executar a pornografia de vingança é punir a vítima, constrangendo-a com a exposição de fotos, vídeos e até áudios íntimos, agredi-la moralmente, violando a sua reputação, honra e liberdade sexual. Resultando em transtornos e danos que afetam as vítimas psicologicamente, emocionalmente e também trazendo danos materiais.

Um exemplo é o caso de Júlia Rebeca dos Santos, que em 2013 se suicidou após a exposição de um vídeo íntimo onde ela praticava sexo com outros dois garotos. A vítima estava postando há alguns dias sua angústia com o caso, mas a família só soube do ocorrido após a sua morte.

Figura 2 – Post feito por Júlia em seu Instagram



Fonte: Magno (2013).

Por não ter uma lei específica tipificando a conduta, os tribunais entendiam os casos como difamação e injúria, de acordo com a primeira decisão julgada pelo TJ do Paraná acerca da apelação criminal nº 756.367-3:

PENAL. APELAÇÃO. CRIMES DE INJÚRIA E DE DIFAMAÇÃO. ARTS. 139 E 140 DO CÓDIGO PENAL. AGENTE QUE POSTA E DIVULGA FOTOS ÍNTIMAS DA EX-NAMORADA NA INTERNET. IMAGENS E TEXTOS POSTADOS DE MODO A RETRATÁ-LA COMO PROSTITUTA EXPONDO-SE PARA ANGARIAR CLIENTES E PROGRAMAS. PROVA PERICIAL QUE COMPROVOU A GUARDA NO COMPUTADOR DO AGENTE, DO MATERIAL FOTOGRÁFICO E A ORIGEM DAS POSTAGENS, BEM COMO A CRIAÇÃO E ADMINISTRAÇÃO DE BLOG COM O NOME DA VÍTIMA. CONDUTA QUE VISAVA A DESTRUIR A REPUTAÇÃO E DENEGRIR A DIGNIDADE DA VÍTIMA. AUTORIA E MATERIALIDADE COMPROVADAS. CONDENAÇÃO CONFIRMADA. RECURSO NÃO PROVIDO. 1. O defeito da procuração outorgada pelo querelante ao seu advogado, para propor queixa-crime, sem 1 Em substituição ao Desembargador José Maurício Pinto de Almeida. TRIBUNAL DE JUSTIÇA Apelação Criminal nº 756.367-3 menção do fato criminoso, constitui hipótese de ilegitimidade do representante da parte, que, a teor do art. 568 C.Pr.Pen., "poderá ser a todo o tempo sanada, mediante ratificação dos atos processuais"... (STF-1ª Turma, HC 86.994-7/RJ, Rel. Min. Sepúlveda Pertence, julg. 14.03.2006, DJ 31.03.2006, p. 18) 2. "1. A ausência de menção ao fato criminoso na procuração que acompanha a queixa trata-se de vício que pode ser sanado a qualquer tempo do processo-crime, ainda que ultrapassado o prazo decadencial, até o momento da sentença final, consoante o disposto no art. 569 do Código de Processo Penal. 2. Qualquer forma de demonstrar o interesse do querelante na persecução criminal quanto ao seu fato objeto

supre o defeito do art. 44 do Estatuto Repressivo, eis que este se foca na possibilidade de futura responsabilização do querelante no caso de cometimento do crime de denúncia caluniosa." (Acórdão nº 24.993, da 2ª C.Criminal do TJPR, Rel. Des. José Maurício Pinto de Almeida, julg. 06.08.2009 - unânime, DJ 28.08.2009) 3. Comete os crimes de difamação e de injúria qualificadas pelo emprego de meio que facilita a sua propagação - arts. 139 e 140, c.c. 141, II do CP - o agente que posta na Internet imagens eróticas e não autorizadas de ex-namorada, bem como textos fazendo-a passar por prostituta. TRIBUNAL DE JUSTIÇA Apelação Criminal nº 756.367-3 (TJ-PR, 2011).

Neste caso, o agressor foi condenado nos crimes previstos nos artigos 139, 140, c/c com os arts. 141, III e 71 e na forma do art. 70, todos do Código Penal, fixando-se a pena em 1 ano, 11 meses e 20 de detenção, iniciando com regime aberto para cumprimento da pena.

Nossa Constituição Federal assegura que tais condutas ferem os direitos constitucionais elencados no art. 5, X da CF/88: "são invioláveis: X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;".

Recentemente, foi sancionada a Lei 13.718/2018 que alterou o Código Penal e considera como crime a propagação de fotos, vídeos ou qualquer outro material com conteúdo sexual sem permissão da vítima, a Lei possui a seguinte redação:

Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:

Portanto, o Direito Penal considera como crime a propagação de fotos, vídeos ou qualquer outro material com conteúdo sexual sem permissão dos participantes, podendo ainda ser passível de indenização no Direito Civil Brasileiro por dano moral e material.

3.2.5 Fake news

Durante as eleições deste ano, foi evidenciado um problema já presente no ambiente virtual, a disseminação de notícias falsas. Assim como na eleição do ano passado nos Estados Unidos, a eleição no Brasil trouxe o debate sobre a relações entre a disseminação de notícias falsas e a democracia. É notório que o impacto

causado pela implantação dessas notícias na internet é potencialmente mais amplo do que as chamadas “focacas” do dia a dia.

Recentemente, Michelle Bachelet, Chefe da ONU, falou sobre os riscos da manipulação de dados coletados na Internet e citou o Brasil como exemplo de como a “desinformação” influenciou as eleições, conforme aponta matéria do Estadão (CHADE, 2018).

Antes do Marco Civil da Internet, tínhamos uma responsabilidade civil subjetiva pelos danos causados por conteúdos publicados em redes sociais e/ou disseminados na Internet. Após vigência do Marco Civil, foi incluso a responsabilidade de remoção desses conteúdos ao provedor e responsáveis pelas redes sociais, após notificação judicial, conforme Art. 19 do Marco Civil:

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.

Atento ao assunto, O TSE criou um fórum com o tema: “Internet e Eleições: um desafio multidisciplinar” para combater a disseminação de *fake news* nas eleições deste ano, editando várias resoluções sobre regras das Eleições Gerais de 2018 em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações e o Comitê Gestor da Internet.

Para o combate da problemática, foi apresentado o projeto de lei PL 6812/2017 onde dispõe sobre a “tipificação criminal da divulgação ou compartilhamento de informação falsa ou incompleta na rede mundial de computadores, que ainda aguarda, conforme consulta realizada no site do Câmara Federal, parecer do Relator na Comissão de Ciência e Tecnologia.

Uma das dificuldades na tipificação desta conduta é a identificação do autor que realmente disseminou a informação e ainda mais complicado encontrar as pessoas que compartilharam as notícias. A forma mais utilizada para disseminação dessas notícias foi através do aplicativo WhatsApp, que utiliza criptografia para proteção de suas conversas.

4 DIREITO COMPARADO

Como observado nos crimes expostos anteriormente, alguns destes delitos são enquadrados em legislações existentes em nosso ordenamento jurídico. Enquanto outros, foram criadas leis específicas que auxiliam no combate e prevenção dessas condutas. Com relação ao cenário internacional, percebemos que o tema é tratado diferente.

Nos Estados Unidos, baseado no modelo Common Law e tendo a política do federalismo implantado em seu território, encontramos um forte combate à criminalidade informática já em 1981, quando fora criada a Lei de Proteção aos Sistemas de Computadores, que determina como crimes o uso de computadores com objetivo de praticar fraudes, furtos ou apropriação indébita. E a principal lei sobre a responsabilidade criminal dessas condutas é a Lei de Fraude e Abuso Computacional, de 1986, com intuito de proteger a acessibilidade dos sistemas para a obtenção de segredos nacionais.

Portugal possui legislação própria contra crimes informáticos – a chamada Lei de Criminalidade Informática, Lei nº 109/91, de 17 de agosto, que prevê conceitos, punições e tipifica várias condutas realizadas no ambiente virtual. Se mostrando bem à frente do Brasil, que possui vários projetos de lei ainda aguardando aprovação no Senado Federal e Câmara de Deputados.

A Convenção de Budapeste, um tratado internacional elaborado em 2001 sobre crimes cibernéticos, foi assinado com objetivo de permitir a cooperação entre os países para obtenção de provas digitais e harmonizar as legislações penal e processo penal. Importante destacar que mesmo diante da importância da aludida convenção, o Brasil não é signatário desta. Entretanto, por ser a única que trata sobre crimes cibernéticos, pode servir de modelo para as demais legislações. De acordo com o documento, os objetivos da Convenção (BOITEUX, 2004, p.172) eram:

Harmonizar as legislações penais substantivas, elementos do delito e outras provisões conexas sobre delitos de informática; promover alterações nas legislações processuais nacionais de forma a conceder poderes de investigação e persecução criminal necessários para combater delitos praticados com o uso de sistemas de computador, ou nos demais tipos de delitos nos quais as provas devam ser obtidas mediante meios eletrônicos e estabelecer um

regime rápido e efetivo de cooperação internacional.

5 CONSIDERAÇÕES FINAIS

No presente artigo, buscou-se apresentar a evolução da internet desde o avanço tecnológico do surgimento dos computadores à difusão pelo mundo, conceituando e apresentando o surgimento e as formas dos crimes virtuais e como o Direito Penal se posiciona frente a tais delitos, demonstrando que a globalização em seus diversos aspectos, trouxe simultaneamente um avanço no número de crimes.

Foram abordados os principais delitos e condutas que já estão previstas em nossa legislação, analisando a necessidade de criação de leis específicas para o combate dessas condutas. Verifica-se ainda que há dispositivos em nossa legislação que preveem a proteção de dados informáticos no Código Penal, acrescentados pela Lei batizada como Lei Carolina Dieckmann, constituindo um avanço importante na tipificação de crimes cibernéticos.

As decisões de alguns tribunais quanto às condutas de pornografia de vingança geram um sentimento de impunidade, já que não haviam leis específicas para apoiar as vítimas e combater os autores dessas agressões. Nota-se a enorme necessidade de criação de leis que definissem as condutas criminosas praticadas no ambiente virtual para evitar o aumento no número de casos, pois a forma em que estavam sendo punidos os agressores era muito branda frente as consequências causadas na vida das vítimas, devendo a pena ser proporcional ao resultado danoso produzido.

Um outro problema encontrado nos crimes cibernéticos é o conhecimento da autoria. Não é possível encontrar visualmente o usuário que estava utilizando determinado computador, e sim o IP da máquina, dificultando em muitos casos a identificação pessoal do infrator, já que estes por muitas vezes aproveitam do anonimato presente nesse ambiente. Neste sentido, se faz extremamente necessária a cooperação dos provedores nas investigações.

Conclui-se que, mesmo diante de tantas lacunas, oportunidades de avanço legislativo e assombrosos números de crimes neste ambiente, quando localizados os criminosos são punidos. O que gera a enorme sensação de impunidade é a dificuldade enfrentada pelo judiciário para punir, a identificação do criminoso e a comprovação da materialidade e autoria dos delitos.

Por fim, é perceptível que medidas de proteção e segurança devem sempre ser vistas e tomadas pelo Estado, que deve assegurar e intervir no que for necessário para que a internet não seja utilizada para práticas criminosas e prejudiciais a seus usuários, atrelando isto, deve capacitar a polícia investigativa, investir em equipamentos e tecnologia para auxiliar o papel do Ministério Público na prática do procedimento penal.

REFERÊNCIAS

BOITEUX, Luciana. Crimes informáticos: reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**, São Paulo, 2004.

BRASIL. **Constituição Federal de 1988**. Promulgada em 5 de outubro de 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 9 out. 2018.

BRASIL. **Lei n. 12.737, de 30/11/2012**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 10 out. 2018.

BRASIL. **Lei n. 13.718, de 24/09/2018**. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm>. Acesso em: 13 nov. 2018.

BRASIL. **Lei n.12.965, de 23/04/14**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 9 out. 2018.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. Apelação Criminal no 0032404-70.2012.8.07.0016. Relator: Desembargador João Batista Teixeira. 3ª Turma Criminal. Brasília, DF, 07 de agosto de 2014. **Diário da Justiça Eletrônico**, 15 de agosto de 2014. p. 276.

CARVALHO, Marcelo Sávio Revoredo Meneze. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança**. Rio de Janeiro, 2006. Dissertação (Mestrado) – Universidade Federal do Rio de Janeiro, COPPE, Rio de Janeiro, 2006.

CASO JÚLIA REBECA. Disponível em:

<<http://www.portalsaibamais.com/novo/2013/11/jovem-tira-a-propria-vida-depois-de-descobrir-que-video-intimo-vazou-na-internet-em-parnaiba/>>. Acesso em: 12 nov. 2018.

CHADE, Jamil. Chefe da ONU cita Brasil como exemplo de eleição afetada por 'desinformação' **Estado**, 14 nov. 2018 Disponível em:

<<https://politica.estadao.com.br/noticias/geral,chefe-da-onu-cita-brasil-como-exemplo-de-eleicao-afetada-por-desinformacao,70002608330>>. Acesso em 14 de out. 2018.

COLARES, Rodrigo Guimarães. Cybercrimes: os crimes na era da informática. **Jus Navigandi**, Teresina, ano 6, n. 59, out. 2002. Disponível em:

<<https://jus.com.br/artigos/3271/cybercrimes-os-crimes-na-era-da-informatica>>. Acesso em: 10 ago. 2018.

CRESPO, Marcelo Xavier. **Diretivas internacionais e direito estrangeiro: crimes digitais**. São Paulo: Saraiva, 2011.

CRESPO, Marcelo Xavier. Revenge Porn: a pornografia da vingança. **JUSBRASIL**. Disponível em: <<https://marcelocrespo1.jusbrasil.com.br/artigos/153948423/revenge-porn-a-pornografia-da-vinganca>> Acesso em 12 de nov 2018.

CRIMES NA INTERNET: falta de normatização, dificuldades na regulamentação e entendimentos sobre o assunto. **JusBrasil**. Disponível em:

<<https://mikhail.jusbrasil.com.br/artigos/234313175/crimes-na-internet-falta-denormatizacao-dificuldades-na-regulamentacao-e-entendimentos-sobre-o-assunto>>. Acesso em: 5 de nov. 2018.

DE OLHO NA SEGURANÇA: **Brasil é o segundo país no mundo com maior número de crimes cibernéticos**. Disponível em

<<https://tecnologia.uol.com.br/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm>>. Acesso em: 30 out. 2018.

DIANA, Daniela. História e Evolução dos Computadores. **Toda Matéria**, 2017.

Disponível em: <<https://www.todamateria.com.br/historia-e-evolucao-dos-computadores/>>. Acesso em: 16 nov. 2018.

EDWARDS, Paul N. **The Closed World**. Cambridge. MA: MIT Press, 1996.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas, SP: Millennium, 2005.

MAGNO, Carlos. Jovem Tira A Própria Vida Depois De Descobrir Que Vídeo Íntimo Vazou Na Internet Em Parnaíba. **Portal Saiba Mais**, nov. 2013. Disponível em: <<http://www.portalsaibamais.com/novo/2013/11/jovem-tira-a-propria-vida-depois-de-descobrir-que-video-intimo-vazou-na-internet-em-parnaiba/>>. Acesso em: 16 nov. 2018.

O I Seminário do Fórum Internet e Eleições, realizado pelo Tribunal Superior Eleitoral (TSE). Disponível em <<http://www.tse.jus.br/imprensa/noticias-tse/2017/Dezembro/especialistas-de-diferentes-setores-da-sociedade-debatem-fake-news-midia-eleicoes-e-redes-sociais-durante-seminario-no-tse>>. Acesso em: 8 de nov. 2018.

ROQUE, Sérgio Marcos. **Criminalidade informática: crimes e criminosos do computador**. São Paulo: ADPESP Cultural, 2007.

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002.

SCHECHTER, Luis Menasche. **A Vida e o Legado de Alan Turing para a Ciência**. Publicado pelo Departamento de Ciência da Computação/UFRJ, 2016. Disponível em <<http://www.dcc.ufrj.br/~luisms/turing/Seminarios.pdf>>. Acesso em: 7 out. 2018.

SUPREMO TRIBUNAL FEDERAL (STF). **Ag. Reg. nos Emb. Div. no Ag. Reg. no Agravo de Instrumento 840.355 Santa Catarina**. Relator: Ministro Dias Toffoli. Disponível em: <file:///C:/Users/larissacosta/Downloads/texto_309505008.pdf>. Acesso em: 16 nov. 2018.

TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico: doutrina, jurisprudência e prática**. São Paulo: Saraiva, 2014.

TRIBUNAL DE JUSTIÇA DO PARANÁ (TJPR). 2. Câmara Criminal. ACR: 7563673 PR 0756367-3. Relator Lilian Romero. Data de Julgamento: 07/07/2011, Data de Publicação: **DJ: 681** Disponível em: <<https://tj-pr.jusbrasil.com.br/jurisprudencia/20132845/apelacao-crime-acr-7563673-pr-0756367-3/inteiro-teor-20132846>>. Acesso em: 16 nov. 2018.

ZANELATO, Marco Antônio. Condutas Ilícitas na sociedade digital. **Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet**, n. IV, p. 173, jul. 2002.