BRASÍLIA 2022

CADERNO DE PÓS-GRADUAÇÃO EM DIREITO

CRIMES DIGITAIS

COORDENAÇÃO

LILIAN ROSE LEMOS ROCHA

ORGANIZAÇÃO

NAIARA FERREIRA MARTINS
LARISSA RODRIGUES DE OLIVEIRA
ANA CAROLINA RODRIGUES DE SOUZA SILVA
JOSÉ RAMALHO BRASILEIRO JÚNIOR
PAULO BINICHESKI

CEUB
EDUCAÇÃO SUPERIOR

Coordenação
Lilian Rose Lemos Rocha

CADERNO DE PÓS-GRADUAÇÃO EM DIREITO

CRIMES DIGITAIS

Organização
Naiara Ferreira Martins
Larissa Rodrigues de Oliveira
Ana Carolina Rodrigues de Souza Filho
José Ramalho Brasileiro Junior
Paulo Binicheski

Brasília
2022

CEUB

ICPD Instituto CEUB de Pesquisa e Desenvolvimento

CENTRO UNIVERSITÁRIO DE BRASÍLIA - CEUB
Reitor
Getúlio Américo Moreira Lopes

INSTITUTO CEUB DE PESQUISA E DESENVOLVIMENTO - ICPD
Diretor
João Herculino de Souza Lopes Filho
Diretor Técnico
Rafael Aragão Souza Lopes

Diagramação
Biblioteca Reitor João Herculino

Capa
CEUB

Documento disponível no link
repositorio.uniceub.br

Dados Internacionais de Catalogação na Publicação (CIP)

Caderno de pós-graduação em direito: crimes digitais / coordenador, Lilian Rose Lemos Rocha – Brasília: CEUB: ICPD, 2022.

231 p.

ISBN 978-85-7267-063-0

1. Direito digital. I. Centro Universitário de Brasília. II. Título.

CDU 34:004.541

Ficha catalográfica elaborada pela Biblioteca Reitor João Herculino

Centro Universitário de Brasília – CEUB
SEPN 707/709 Campus do CEUB
Tel. (61) 3966-1335 / 3966-1336

PREFÁCIO

Pioneirismo sempre foi uma característica do UniCEUB; outra característica é a evolução permanente. A Instituição sempre acompanhou a evolução tecnológica e pedagógica do ensino. Isso se coaduna com a filosofia institucional que é a de preparar o homem integral por meio da busca do conhecimento e da verdade, assegurando-lhe a compreensão adequada de si mesmo e de sua responsabilidade social e profissional. Destarte, a missão institucional é a de gerar, sistematizar e disseminar o conhecimento visando à formação de cidadãos reflexivos e empreendedores, comprometidos com o desenvolvimento socioeconômico sustentável.

E não poderia ser diferente. Com a expansão do conteúdo acadêmico que se transpassa do físico para o virtual, do local para o universal, do restrito para o difundido, isso porque o papel não é mais apenas uma substância constituída por elementos fibrosos de origem vegetal, os quais formam uma pasta que se faz secar sob a forma de folhas delgadas donde se cria, modifica, transforma letras em palavras; palavras em textos; textos em conhecimento, não! O papel se virtualiza, se desenvolve, agora, no infinito, rebuscado de informações. Assim, o UniCEUB acompanha essa evolução. É dessa forma que se desafia o leitor a compreender a atualidade, com a fonte que ora se entrega à leitura virtual, chamada de ebook.

Isso é resultado do esforço permanente, da incorporação da ciência desenvolvida no ambiente acadêmico, cujo resultado desperta emoção, um sentimento de beleza de que o conteúdo científico representa o diferencial profissional.

Portanto, convido-os a leitura desta obra, que reúne uma sucessão de artigos que são apresentados com grande presteza e maestria; com conteúdo forte e impactante; com sentimento e método, frutos da excelência acadêmica.

João Herculino de Souza Lopes Filho
Diretor ICPD/UniCEUB

APRESENTAÇÃO

Os artigos acadêmicos apresentados no presente livro são frutos da disciplina Crimes Digitais, ministrada no terceiro bimestre de 2021 pelo Professor Dr. Paulo Binicheski.

Foram selecionados artigos sobre os textos trabalhados durante o bimestre. Os textos são de autoria das e dos discentes da disciplina, sendo elas e eles: Camila Pereira Dias, Déborah Boechat Côrrea Lima, Édio Henrique de Almeida José e Azevedo, Eduardo Oesterreich da Rosa, Gabriella Navarro de Azevedo Pinheiro, Isabelly Alves de Melo, Letícia de Amorim Pereira, Maycon Douglas de Miranda Silva, Mariana Guimarães Dourado, Natália Rocha Damasceno, Nathan Vinagre Augusto dos Santos e Samanta Bárbara Ribeiro do Nascimento.

SUMÁRIO

ANÁLISE DA TEORIA DA CEGUEIRA DELIBERADA EM CRIMES DE CYBER-LAVAGEM

Camila Pereira Dias[1]

RESUMO

Este presente estudo teve como objetivo principal uma análise breve do desenvolvimento evolutivo e jurídico que levou a institucionalização da teoria da cegueira deliberada, bem como os crimes digitais a qual é empregada, para enfim, compreender e fazer a identificação da sua aplicabilidade em casos concretos no ordenamento jurídico brasileiro no âmbito do direito penal e processo penal. A metodologia que foi adotada é a do método bibliográfico. Assim, foram examinadas para elaboração do presente trabalho, as bibliografias de doutrinadores nacionais que se encontravam disponíveis que tratam o direito penal como um todo, e em doutrinas que abordam especificamente sobre o tema, que é a área de concentração deste trabalho, bem como jurisprudências e sítios eletrônicos que se amoldavam ao tema. A abordagem qualitativa do estudo foi adotada em função da aderência e coerência que possui em relação aos objetivos desta pesquisa, o que permite a compreensão da presente problemática frente ao ordenamento jurídico atual.

Palavras-chave: Origem. Teoria da cegueira deliberada. Crimes Digitais.

ABSTRACT

This present study had as its main objective a brief analysis of the evolutionary and legal development that led to the institutionalization of the theory of deliberate blindness, as well as digital crimes, which is used, finally, to understand and identify its applicability in concrete cases in the Brazilian legal system in the scope of criminal law and criminal procedure. The methodology that was adopted is the bibliographic method. Thus, the bibliographies of national scholars that were available that deal with criminal law as a whole, and in doctrines that specifically address the subject, which is the area of concentration of this work, as well as jurisprudence, were examined for the preparation of this work. and electronic sites that fit the theme. The qualitative approach of the study was adopted due to its adherence and coherence in relation to the objectives of this research,

[1] Bacharel em Direito pelo Centro Universitário Projeção, 2017. Aluna do curso de pós-graduação *lato senso* em Direito Penal e Controle Social, Centro Universitário de Brasília - UniCEUB/ICPD. Email: mila.p.dias@sempreceub.com.

which allows for an understanding of the present problem in light of the current legal system.

Keywords: Source. Theory of deliberate blindness. Digital criminals.

1 INTRODUÇÃO

O presente texto, em um primeiro momento, foi abordado e desenvolvido sobre a ótica do processo histórico e criacionista que deu a origem da teoria da cegueira deliberada e a sua evolução. Por fim, são apresentadas e analisadas as decisões brasileiras que a venham levando em consideração para sua utilização como respaldo decisório em vários crimes, uma vez que a cada segundo esta matéria se encontra mais pertencente e comum aos dias atuais.

Tal estudo mostra-se relevante haja vista que com o aumento dos procedimentos investigatórios e cooperações internacionais, vários crimes acabam sendo constantemente descobertos, tendo em vista que as suas práticas vêm a ocorrer no decorrer dos anos de forma deliberada e tomam grande repercussão.

Deste modo, em consequência à sua utilização como fundamentação em decisões que vieram a tratar de crimes em geral, bem como, os crimes contra a administração pública brasileira, por exemplo, o de lavagem de dinheiro, cresce consideravelmente as ações solucionadas satisfatoriamente das quais tratam sobre eventuais crimes, tendo em vista que estas determinadas condutas criminosas possuem de alguma forma os elementos essenciais que são levados em consideração para a aplicabilidade dessa teoria.

2 PROCESSO EVOLUTIVO

A possibilidade de o julgador utilizar-se de uma teoria como fundamento decisório é uma das grandes garantias de evolução jurídica, mas qual é o significado terminológico, filosófico e jurídico da palavra teoria?

Segundo o dicionário Michaelis[2], o primeiro termo apresentado do significado de teoria traz que esta é o "conjunto de princípios, regras ou leis, aplicados a uma área, ou mais geralmente a uma arte ou ciência", bem como na

[2] MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa**. Disponível em <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=teoria> Acesso em: 29 de set. de 2021.

mesma bibliografia, o quinto significado traz de forma mais filosófica que teoria se dá diante ao "conjunto de conhecimentos sistematizados que se fundamentam em observações empíricas e em estudos racionais e que, ao formular leis e categoria gerais, possibilitam classificar, ordenar e interpretar os fatos e as realidades da natureza."

Assim, pode ser compreendido na área jurídica acerca dos significados acima apresentados, que a conceituação de Teoria se dá pela criação de uma norma doutrinária decorrente de um aglomerado de fatores, diante da ação ou omissão, e que levam a justificar determinada conduta em matéria específica.

Deste modo, observadas as concepções acima, teve-se a criação de várias teorias no ordenamento jurídico, mas devido a decorrência de alguns fatores, neste caso a omissão destes, uma vez que em matéria criminal, alguns indivíduos se botavam em estado de ignorância quanto a origem dos valores e/ou bens, originou-se então a Teoria da Cegueira Deliberada na Inglaterra no século XIX.[3]

Conforme Monteiro[4], a Teoria da Cegueira Deliberada se caracteriza quando o agente aparenta estar em estado de cegueira a determinados fatos ilícitos quanto à origem de bens, direitos ou até mesmo valores, a fim de auferir vantagem sobre eles se valendo da omissão destas informações quanto a sua inércia frente comunicação a autoridades competentes.

Outrora, esta teoria também pode ser conhecida como Teoria do Avestruz[5], uma vez que aquele agente que se vale dessa inobservância ilícita, assemelha-se ao Avestruz, que é um animal de hábitos peculiares e possui como característica o

[3] LIMA, Milka Patricia Vinhal de. A admissibilidade do dolo eventual e a aplicabilidade da cegueira deliberada no crime de lavagem de dinheiro: 2014. 54f. Monografia (Graduação) –Centro Universitário de Brasília, Brasília, 2014. Disponível em: http://www.repositorio.uniceub.br/handle/235/5996. Acesso em: 29 de set. de 2021.

[4] MONTEIRO, Taiana Alves. **Aplicação da Teoria da Cegueira Deliberada no Brasil**. Disponível em: <http://www.conjur.com.br/2009-set-28/necessario-dolo-especifico-caracterizacao-corrupcao-eleitoral>. Acesso em: 29 de set. de 2021.

[5] PEREIRA, Mateus Henrique Chaves. A aplicabilidade da teoria da cegueira deliberada e o dolo eventual aos crimes de lavagem de dinheiro. 2018.54f. Monografia (Graduação) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2018. Disponível em: <https://repositorio.uniceub.br/jspui/handle/235/12570> Acesso em: 29 de set. de 2021.

rebaixamento de sua cabeça até o chão como estratégia de camuflagem achando que agindo dessa forma vai obter vantagem quanto aos seus predadores.[6]

Na época do desenvolvimento desta teoria, existiam predominantemente no mundo dois sistemas jurídicos, o *Common Law* e o *Civil Law*, nos quais um se baseia na lei e costumes, e o outro somente na lei.

A teoria teve sua aplicabilidade inicial no sistema *Commom Law*, uma vez que esta decorreu de ações que não havia exatamente previsão legal específica no ordenamento jurídico do sistema na qual, por exemplo, a Inglaterra desde o Século XIII utilizava para reger o seu território. Esse sistema se baseia no direito costumeiro vinculado as decisões judiciais, com a finalidade de evitar contradições posteriores. Nesse tocante o jurista Campos[7] descreve como se dava o procedimento da utilização de um direito costumeiro pelos magistrados no sistema *Common Law:*

> Cabia ao magistrado a tarefa de verbalizar tais regras quando fosse apreciar os acontecimentos fáticos dos casos que lhe são submetidos. Desta forma, ele apenas verbalizaria, por meio de uma construção teórica logicamente coerente, a regra de direito já utilizada. A partir disso, a regra passa a ser utilizada pelos juízes dos casos seguintes, aplicando, deste modo, o precedente.

Posteriormente, a Suprema Corte dos Estados Unidos viu-se a necessidade da arguição da Teoria da Cegueira Deliberada (*willful blindness doctrine*) para aplicação desta em casos semelhantes e posteriores ao de um vendedor de carros, que fazia venda de veículos furtados ou roubados, assim como mencionado a jurista Monteiro[8], mas no fim do processo não se comprovou que sabia que os veículos eram frutos de práticas ilícitos.

No entanto, os legisladores dos Estados Unidos ainda se encontravam em questionamentos sobre a institucionalização da Teoria e passaram a analisá-la com

---

[6] GRUPO ABRIL. **O avestruz enterra a cabeça quando fica com muito medo.** Disponível em: <https://super.abril.com.br/ciencia/o-avestruz-enterra-a-cabeca-quando-fica-com-muito-medo/> Acesso em: 29 de set. de 2021

[7] CAMPOS, Fernando Teófilo. Sistemas de Common Law e de Civil Law: conceitos, diferenças e aplicações: Breves apontamentos sobre os Sistemas de Common Law e de Civil Law. Disponível em:<https://jus.com.br/artigos/62799/sistemas-de-common-law-e-de-civil-law-conceitos-diferencas-e-aplicacoes> Acesso em: 29 de set. de 2021.

[8] MONTEIRO, Taiana Alves. **Aplicação da Teoria da Cegueira Deliberada no Brasil**. Disponível em: <http://www.conjur.com.br/2009-set-28/necessario-dolo-especifico-caracterizacao-corrupcao-eleitoral>. Acesso em: 29 de set. de 2021

mais afinco, uma vez que para que essa possa ser aplicada há a necessidade de que o agente tenha conhecimento de que aqueles valores ou bens são decorrentes de práticas ilícitas para se caracterizar o dolo e em decorrência disso nos EUA naquela época não se admitia dolo eventual em crimes de lavagem de capitais.

Diante aos fatores inerentes a evolução da Teoria da Cegueira Deliberada e apesar da criação desta teoria ter sido realizada nos países que utilizam o Commom Law frente a casos decorrentes naquele território, esta ensejou vários questionamentos quanto a sua aplicação em outros países que utilizavam do Civil Law em seu ordenamento jurídico.

Assim, o doutrinador Castro[9] aduz que o Sistema Jurídico *Civil Law*

> (...) caracteriza-se pelo fato de as leis serem a pedra primal da igualdade e da liberdade, posto que objetivava proibir o juiz de lançar interpretação sobre a letra da lei, fornecendo, para tanto, o que se considerava como sendo uma legislação clara e completa; onde, ao magistrado, caberia apenas proceder à subsunção da norma.

Deste modo, percebeu-se que o Civil Law se demonstra presente nos países que utilizam como fonte norteadora as leis e que estas só serão adotadas desde que criadas pelo Poder Legislativo, mesmo que de forma genérica e abstrata venha falar dos fatos na qual será aplicada, apesar da existência das demais fontes do direito que abrangem os princípios de forma geral, as doutrinas e as jurisprudências.[10]

Os órgãos julgadores brasileiros possuíam várias divergências quanto a sua utilização em casos de responsabilização penal, uma vez que no ordenamento jurídico brasileiro, precisamente no Artigo 5º, inciso II, da Constituição Federal da República Federativa do Brasil[11] aduz que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei." Ou seja, só poderá ser aplicada sanção penal que esteja tipificada no Direito Penal Brasileiro.

No entanto, o Brasil mesmo que possuindo um ordenamento jurídico diferente do *Common Law,* bem como aos de outros países, a Teoria da "Cegueira"

[9] CASTRO, Guilherme Fortes Monteiro de; GONÇALVES, Eduardo da Silva. **A aplicação da C*ommon law* no Brasil: diferenças e afinidades.**
[10] CAMPOS, Fernando Teófilo. **Sistemas de *Common Law* e de *Civil Law***: conceitos, diferenças e aplicações**:** Breves apontamentos sobre os Sistemas de *Common Law* e de *Civil Law*.
[11] BRASIL. **Constituição Federal da República Federativa do Brasil.**

Deliberada ou a Teoria do Avestruz começou a ter espaço em casos do Direito Penal, dada a necessidade de aplicação em determinados casos in concreto e diante disso o jurista Freitas[12] ponderou que

> (...)trata-se de crescente aproximação entre institutos e políticas existentes no sistema jurídico vigorante em países anglo-saxões (sistema common law) e no sistema adotado em países da Europa continental e da América Latina (sistema civil law), ainda que os mesmos se diferenciem basicamente pela preponderância distintamente atribuída. A integração econômica entre as nações provocou a busca pela integração dos respectivos ordenamentos jurídicos nacionais e acarretou a reconfiguração dos sistemas de fontes com vistas a alcançar um Direito Penal, se não universal ao menos harmônico. Registra-se desde já o fato de haver resistência de uma parcela da doutrina quanto à rapidez e acriticismo com os quais, supostamente, têm sido acolhidos alguns anglicanismos, institutos (whistleblowing, compliance programs, gatekeepers, willfull blindness theory), regramentos como a as recomendações do Grupo de Ação Financeira Internacional – GAFI e, num prisma geral, a própria política criminal ostentada e fomentada por países desenvolvidos. Tal posicionamento de internacionalização do Direito Penal incorporaria, em larga medida, 16 uma proposta elaborada por aqueles países para impor seus anseios político-criminais e de seus próprios sistemas de fontes do Direito. Respeitado o posicionamento citado, crê-se que não devem ser desprezadas as experiências advindas da realidade jurídica estrangeira e as marcadas distinções entre sistemas jurídicos não constituem obstáculos intransponíveis nesse processo.

Deste modo, em observância as recomendações do GAFI e a necessidade de penalização a agentes que auferem vantagens quanto a inobservância ilícita da origem dos produtos, o Brasil, passou a utilizar-se da Teoria da "Cegueira" Deliberada para fundamentar decisões que anteriormente não poderiam ser solucionadas.

3 CYBER-LAVAGEM

A tecnologia vem trazendo para a sociedade elementos inovadores e dinâmicos, os quais destacaram-se pelo surgimento das moedas virtuais ou cyber-moedas no mercado financeiro mundial criadas por particulares como novo meio de circulação de riquezas.

[12] FREITAS, Rafael Sbeghen. **A Aplicabilidade da Teoria da "Cegueira" Deliberada ao Delito de Lavagem de Capitais no Brasil**.

> As chamadas "moedas virtuais" ou "moedas criptográficas" são representações digitais de valor que não são emitidas por Banco Central ou outra autoridade monetária. O seu valor decorre da confiança depositada nas suas regras de funcionamento e na cadeia de participantes.[13]

No entanto, ainda que as criptomoedas possuam complexa tecnologia, não significa que exista uma efetiva fiscalização, pois o Poder Público desconhece a origem dos bens, uma vez que as moedas digitais são criptografadas e tal tecnologia obstaculiza o rastreamento delas.

Ademais, segundo Andrade[14]

> A criptografia do dinheiro confere às operações virtuais os benefícios de confidencialidade, integridade, rapidez nas transações e autenticação, e foi projetada com base em objetivos que tornam o uso das criptomoedas uma alternativa atrativa para a moeda corrente e, por meio de *softwares* específicos, fornece aos usuários liberdade de pagamento, segurança, taxas muito baixas e menos riscos para comerciantes.

Desta forma, em decorrência da utilização e criação de moedas digitais e a dificuldade em seu rastreamento, pessoas mal-intencionadas as utilizam para praticar atos ilícitos quanto a prática de crimes mediante o uso da internet e a sua facilidade de acesso.

> Os administradores da moeda virtual ou empresas que se dedicam a uma troca de moedas virtuais entre países diferentes podem usar “lavanderias” (um conjunto de serviços que gera um grande número de carteiras e envia moeda entre elas de forma casual) para conferir maior complexidade em suas ações e disfarçar eventuais vestígios. Os sinais de uso de “lavanderias” virtuais são muito semelhantes aos usados em “lavanderias” reais, especialmente porque no ambiente virtual das bitcoins não há regulamentação ou mecanismos de identificação dos usuários independente de criptografia de dados. A moeda digital é descentralizada e sigilosa, o que torna propício o ambiente para a atuação de grupos criminosos.
>
> Os criminosos usam a natureza da transação virtual para esconder as fontes e manipular o lucro sobre as operações realizadas, o que ocorre porque a maioria das operações com

[13] PEREIRA, Luiz Fernando. **O crime de lavagem de dinheiro e as moedas virtuais**. Disponível em: https://www.migalhas.com.br/depeso/298505/o-crime-de-lavagem-de-dinheiro-e-as-moedas-virtuais. Acesso em: 29 set. 2021.

[14] ANDRADE, Mariana Dionísio de. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. **Revista Brasileira Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 43-59

> moedas virtuais não possui contatos no ambiente real e porque há meios de ocultar uma eventual fonte ilegal do dinheiro. Uma categoria de casos de uso de moedas virtuais com fins criminosos inclui o cenário que os criminosos recebem controle sobre contas de usuários legais e a oportunidade de realizar as operações.[15]

4 APLICABILIDADE NO BRASIL

No Brasil, ao decorrer dos anos jurídicos, bem como a necessidade de algumas modificações legislativas, o sistema *Civil Law* e o sistema *Common Law* passaram a estar mais presentes e serem utilizados em uma mesma decisão no sistema jurídico brasileiro.

Assim, a teoria passou a ser analisada com maior profundidade quanto ao ordenamento jurídico pátrio e ficou-se o questionamento se esta poderia ser utilizada de forma culposa ou de maneira análoga ao dolo eventual, quando o agente assume o risco quanto ao resultado. Deste modo, alguns julgadores e doutrinadores, entenderam que esta pode sim equiparar-se ao dolo eventual, bem como, pode ser observado o entendimento do pesquisador e jurista Nascimento citado por Cabral, no qual aduz que:

> Para a teoria da cegueira deliberada o dolo aceito é o eventual. Como o agente procura evitar o conhecimento da origem ilícita dos valores que estão envolvidos na transação comercial, estaria ele incorrendo no dolo eventual, onde prevê o resultado lesivo de sua conduta, mas não se importa com este resultado. Não existe a possibilidade de se aplicar a teoria da cegueira deliberada nos delitos ditos culposos, pois a teoria tem como escopo o dolo eventual, onde o agente finge não enxergar a origem ilícita dos bens, direitos e valores com a intenção de levar vantagem. Tanto o é que, para ser supostamente aplicada a referida teoria aos delitos de lavagem de dinheiro "exige-se a prova de que o agente tenha conhecimento da elevada probabilidade de que os valores eram objeto de crime e que isso lhe seja indiferente." [16]

A teoria foi primeiramente analisada no Brasil no ano de 2008 no processo que veio arguir se havia a responsabilidade de uma concessionária de veículos em

[15] ANDRADE, Mariana Dionísio de. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. **Revista Brasileira Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 43-59

[16] CABRAL, Bruno Fontenele. **Breves comentários sobre a teoria da cegueira deliberada (willful blindness doctrine)**. Disponível em: <https://jus.com.br/artigos/21395/breves-comentarios-sobre-a-teoria-da-cegueira-deliberada-willful-blindness-doctrine> Acesso em: 29 de set. de 2021.

face da venda de 11 veículos, dos quais foram comprados com o dinheiro adquirido no Furto à Caixa-Forte do Banco Central do Brasil situado de Fortaleza.

> PENAL E PROCESSUAL PENAL. FURTO QUALIFICADO À CAIXA-FORTE DO BANCO CENTRAL EM FORTALEZA. IMPUTAÇÃO DE CRIMES CONEXOS DE FORMAÇÃO DE QUADRILHA, FALSA IDENTIDADE, USO DE DOCUMENTO FALSO, **LAVAGEM DE DINHEIRO** E DE POSSE DE ARMA DE USO PROIBIDO OU RESTRITO (...) - No caso dos autos, o grupo que executou os fatos configura uma verdadeira organização criminosa, tendo empreendido esforços, recursos financeiros de monta, inteligências, habilidades e organização de qualidade superior, em uma empreitada criminosa altamente ousada e arriscada. O grupo dispunha de uma bem definida hierarquização com nítida separação de funções, apurado senso de organização, sofisticação nos procedimentos operacionais e nos instrumentos utilizados, acesso a fontes privilegiadas de informações com ligações atuais ou pretéritas ao aparelho do Estado (pelo menos a empregados ou ex-empregados terceirizados) **e um bem definido esquema para posterior branqueamento dos capitais obtidos com a empreitada criminosa antecedente. Reunião de todas as qualificações necessárias à configuração de uma organização criminosa, ainda que incipiente. 2.4- Imputação do crime de lavagem em face da venda, por loja estabelecida em Fortaleza, de 11 veículos, mediante o pagamento em espécie: a transposição da doutrina americana da cegueira deliberada (willful blindness), nos moldes da sentença recorrida, beira, efetivamente, a responsabilidade penal objetiva; não há elementos concretos na sentença recorrida que demonstrem que esses acusados tinham ciência de que os valores por ele recebidos eram de origem ilícita, vinculada ou não a um dos delitos descritos na Lei n.º 9.613/98. O inciso II do PARÁGRAFO 2.º do art. 1.º dessa lei exige a ciência expressa e não, apenas, o dolo eventual. Ausência de indicação ou sequer referência a qualquer atividade enquadrável no inciso IIdo PARAGRAFO 2º. - Não há elementos suficientes, em face do tipo de negociação usualmente realizada com veículos usados, a indicar que houvesse dolo eventual quanto à conduta do art. 1.º, PARÁGRAFO 1º, inciso II, da mesma lei; na verdade, talvez, pudesse ser atribuída aos empresários a falta de maior diligência na negociação (culpa grave), mas não, dolo, pois usualmente os negócios nessa área são realizados de modo informal e com base em confiança construída nos contatos entre as partes.**[17]

[17] _____. Tribunal Regional Federal da 5ª Região. **ACR 5520 CE 0014586-40.2005.4.05.8100**. Desembargador Federal Rogério Fialho Moreira. 09/09/2008. Fonte: Diário da Justiça - Data: 22/10/2008 - Página: 207 - Nº: 205 - Ano: 2008. Disponível em:

Acerca do caso acima, o acórdão foi proferido de forma Unânime e percebeu-se que a referida concessionária não teria como ter conhecimento de que o dinheiro pago em espécie na compra dos veículos era proveniente do furto, uma vez que esta não agiu de forma dolosa, haja vista que no horário da compra não se tinha conhecimento público da ação criminosa ao Banco. Assim, entendeu-se que somente esta agiu com culpa por não possuírem maiores formalidades quanto a venda dos veículos.

Outrora, a teoria da cegueira deliberada foi utilizada para analisar a situação de outros casos que devido à forma empregada na conduta criminosa, ao ato de "fechar os olhos" para atitudes ilegais e a quantidade de pessoas envolvidas, sendo algumas importantes no ramo político e econômico do país, bem como a consequência de uma grande repercussão nacional ou internacional, como o caso do Mensalão, julgado pela Ação Penal 470[18], pelo Supremo Tribunal Federal.

No julgamento do Mensalão, o Supremo Tribunal Federal analisou a teoria em frente as condutas de José Eduardo Cavalcanti de Mendonça, conhecido como Duda Mendonça, e de sua sócia, Zilmar Fernandes da Silveira, mas dadas as alegações que ambos apresentaram, eles foram absolvidos pelo crime de lavagem de dinheiro.

Assim, conforme Pereira, com o Julgamento da Ação Penal 470 os Ministros do Egrégio Supremo Tribunal Federal mantiveram debates acalorados dando o início as descobertas de demais casos de lavagem de capitais no Brasil, e o mesmo órgão reconheceu a necessidade de utilizar a teoria da cegueira deliberada quando se tratar dessas matérias para que possam ser sanadas algumas lacunas na legislação brasileira.[19]

<http://www.jusbrasil.com.br/jurisprudencia/8249976/apelacao-criminal-acr-5520-ce-0014586-4020054058100-trf5>. Acesso em: 29 de set. de 2021.

[18] BRASIL. Supremo Tribunal Federal. Ação Penal 470. Disponível em: <https://www2.stf.jus.br/portalStfInternacional/cms/destaquesNewsletter.php?sigla=newsletterPortalInternacionalNoticias&idConteudo=214544> Acesso em: 29 de set. de 2021.

[19] PEREIRA, Mateus Henrique Chaves. A aplicabilidade da teoria da cegueira deliberada e o dolo eventual aos crimes de lavagem de dinheiro. 2018.54f. Monografia (Graduação) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2018. Disponível em: <https://repositorio.uniceub.br/jspui/handle/235/12570> Acesso em: 29 de set. de 2021.

Deste modo, a Teoria passou a ser maior implementada em julgamentos de matérias que tratam de cunho econômico e financeiro, principalmente os de lavagem de dinheiro[20], porque

> No caso do Brasil, é de ressaltar a mobilização do país em juntar-se à comunidade internacional nesta luta contra a criminalidade. Adotando a recomendação formulada pela Convenção de Viena, e promulgando a Lei 9.613/98 dispondo sobre o crime de lavagem de dinheiro. Esta lei não trata somente do crime de lavagem, mas estabelece também medidas administrativas de prevenção que podem se vistas como mais efetivas em produzir efeitos inibitórios contra a lavagem de dinheiro.[21]

Posteriormente, no dia 17 de março de 2014 iniciou-se a Operação Lava Jato, na qual se teve a repercussão mundial , uma vez que em conjunto com a Polícia Federal do Brasil e o Juiz Sérgio Moro, cumpriram-se vários mandados e consequente condenação de mais de cem pessoas, que participavam de crimes de corrupção ativa e passiva, gestão fraudulenta, lavagem de dinheiro, organização criminosa, obstrução da justiça, operação fraudulenta de câmbio e recebimento de vantagem indevida.

Dentre essas condenações, o Juiz Sergio Moro utilizou-se da aplicação da teoria da cegueira deliberada na Ação Penal que condenou João Cerqueira de Santana Filho e afirmou ainda no processo que o indivíduo que pratica condutas tipificadas como lavagem de capitais, bem como a ocultação ou dissimulação destes, não significa que afasta completamente o dolo da conduta e a sua responsabilidade criminal se dá ao fato de que o indivíduo decidiu manter-se em estado de ignorância quanto a origem dos bens, direitos ou valores envolvidos na transação, mesmo que este tivesse a possibilidade de procurar saber mais sobre estes fatores. [22]

---

[20] BRASIL. Congresso Nacional. Lei n.º 9.613, de 3 de março de 1998 que "dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências." **Disponível** em:< http://www.planalto.gov.br/ccivil_03/LEIS/L9613.htm> Acesso em: Acesso em: 29 de set. de 2021.

[21] COELHO, Edgard Lima. **A Intrínseca Relação entre o Crime de Lavagem de Dinheiro e as Organizações Criminosas.** Caderno de Pós-Graduação Caderno de Pós-graduação em Direito: Compliance e relações governamentais / coordenadores: Lilian Rose Lemos Rocha [et al.] – Brasília: UniCEUB: ICPD, 2019. Disponível em: <https://repositorio.uniceub.br/jspui/handle/prefix/13411> Acesso em: 29 de set. de 2021.

[22] BRASIL. Justiça Federal da 13º Vara Criminal de Curitiba. **Ação Penal nº 5013405-59.2016.4.04.7000/PR** Disponível em: <https://www.conjur.com.br/dl/moro-condena-joao-santana-cegueira.pdf> Acesso em: 29 de set. de 2021.

> Em notícia recente (05/03/19), já temos um caso intrigante no qual facção criminosa utilizava Bitcoin para lavagem de dinheiro6 e que na reportagem o policial disse que, de acordo com um especialista consultado pela PM, esse equipamento é "usado para fazer a lavagem do dinheiro do tráfico" e que eles conseguem até "dobrar o valor da noite para o dia" e também que essas máquinas podem girar em torno de "1 milhão a 2 milhões por dia7". Portanto, trata-se de uma realidade a lavanderia virtual.[23]

A Egrégia Corte do STJ aduz:

> "Sabe-se que para a aplicação da teoria da cegueira deliberada, deve ficar demonstrado no quadro fático apresentado na lide que o agente finge não perceber determinada situação de ilicitude para, a partir daí, alcançar a vantagem pretendida."[24]

Por fim, ainda que tenhamos pouquíssimas discussões dos tribunais, já sabemos pelo menos que a competência para julgamento de ações penais haja vista que o STJ se manifestou que "inexistindo indícios, por ora, da prática de crime de competência federal, o procedimento inquisitivo deve prosseguir na justiça estadual, a fim de que se investigue a prática de outros ilícitos, inclusive estelionato e crime contra a economia popular".[25]

> Quanto em relação à aplicação do dolo eventual é possível inclusive mais próximo de uma identificação do comprador da moeda virtual, como origem o vendedor. Talvez, ao critério de regulamentação normativa seria um cadastramento integro e concentrado por parte do vendedor, no qual terá a obrigatoriedade de apresentar aos órgãos públicos quem são seus compradores de moedas virtuais e um órgão específico fiscalizador poderá inibir as transações eletrônicas.[26]

Recentemente, a Comissão Especial da Câmara dos Deputados, aprovou pena maior para lavagem de dinheiro através de moedas virtuais, assim,

> "(...)aumenta a pena, de um a dois terços, para os crimes de lavagem de dinheiro com o uso de moedas virtuais, como a Bitcoin e outras criptomoedas. Atualmente, a pena para lavagem de dinheiro é de reclusão de três a dez anos e multa.

[23] PEREIRA, Ana Paula. **Facção criminosa utilizava Bitcoin para lavagem de dinheiro, afirma PM de São Paulo**. Disponível em: https://cointelegraph.com.br/news/criminals-used-bitcoin-for-money-laundering-says-sao-paulo-police. Acesso em: 29 set. 2021.

[24] BRASIL. STJ - RECURSO ESPECIAL: REsp 1565832 RJ 2015/0282311-7

[25] BRASIL. STJ - CONFLITO DE COMPETENCIA: CC 161123 SP 2018/0248430-4.

[26] PEREIRA, Mateus Henrique Chaves. A aplicabilidade da teoria da cegueira deliberada e o dolo eventual aos crimes de lavagem de dinheiro. 2018.54f. Monografia (Graduação) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2018. Disponível em: <https://repositorio.uniceub.br/jspui/handle/235/12570> Acesso em: 29 de set. de 2021.

> Com a mudança, a pena aumentaria para reclusão de quatro anos a 16 anos e oito meses, além da multa. A proposta ainda deve ser analisada pelo Plenário da Câmara."[27]

Esta teoria mesmo que aplicada em casos de extenso impacto público e transnacional, ainda se encontra pouco aplicada e estudada em crimes cibernéticos, levando-a a ser utilizada conforme entendimentos doutrinários e jurisprudenciais para que melhor se encaixe aos interesses das partes interessadas em questão, o Poder Público e a coletividade.

5 CONCLUSÃO

O objeto ora estudado no qual abordou a pesquisa sobre o tema "A análise da teoria da cegueira deliberada em crimes de cyber-lavagem", não se encontrou exaurido, contudo, o estudo aqui realizado trouxe a oportunamente a possibilidade de obtenção novos conhecimentos e aperfeiçoamento inerente aos assuntos aqui explanados e elaborados.

Outrora, quanto à falta de disposição legal particularizada ao assunto, leva os magistrados a embasarem suas decisões somente em conformidade aos dispositivos doutrinários e jurisprudenciais, aplicando-se então das regras já normatizadas sobre ao dolo eventual, de forma análoga, uma vez que falta legislação regulamentadora sobre o específico assunto.

Por todo o exposto, sem ter a menor pretensão de esgotar o presente tema, assim observa-se que devem ser propostos novos debates, a fim de que estes possam de forma concisa e coerente trazer novos resultados, bem com, apresentarem seguranças jurídicas quanto ao assunto.

REFERÊNCIAS

ANDRADE, Mariana Dionísio de. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. **Revista Brasileira Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 43-59

[27] BRASIL. Agência Câmara de Notícias. **Comissão aprova pena maior para lavagem de dinheiro com moedas virtuais**. 2021.<https://www.camara.leg.br/noticias/811726-comissao-aprova-pena-maior-para-lavagem-de-dinheiro-com-moedas-virtuais#:~:text=Comiss%C3%A3o%20especial%20da%20C%C3%A2mara%20dos,a%20dez%20anos%20e%20multa>. Acesso em: 29 de set. de 2021.

BRASIL. Agência Câmara de Notícias. **Comissão aprova pena maior para lavagem de dinheiro com moedas virtuais**. 2021.<https://www.camara.leg.br/noticias/811726-comissao-aprova-pena-maior-para-lavagem-de-dinheiro-com-moedas-virtuais#:~:text=Comiss%C3%A3o%20especial%20da%20C%C3%A2mara%20dos,a%20dez%20anos%20e%20multa>. Acesso em: 29 de setembro de 2021.

_____. Congresso Nacional. Lei n.º 9.613, de 3 de março de 1998 que "dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências." Disponível em:< http://www.planalto.gov.br/ccivil_03/LEIS/L9613.htm> Acesso em: Acesso em: 29 de setembro de 2021.

_____. Justiça Federal da 13º Vara Criminal de Curitiba. Ação Penal nº 5013405-59.2016.4.04.7000/PR Disponível em: <https://www.conjur.com.br/dl/moro-condena-joao-santana-cegueira.pdf> Acesso em: 29 de setembro de 2021.

_____. STJ - CONFLITO DE COMPETÊNCIA: CC 161123 SP 2018/0248430-4. Acesso em: 29 de setembro de 2021.

_____. STJ - RECURSO ESPECIAL: REsp 1565832 RJ 2015/0282311-7. Acesso em: 29 de setembro de 2021.

_____. Supremo Tribunal Federal. Ação Penal 470. Disponível em: <https://www2.stf.jus.br/portalStfInternacional/cms/destaquesNewsletter.php?sigla=newsletterPortalInternacionalNoticias&idConteudo=214544> Acesso em: 29 de setembro de 2021.

_____. Tribunal Regional Federal da 5ª Região. **ACR 5520 CE 0014586-40.2005.4.05.8100**. Desembargador Federal Rogério Fialho Moreira. 09/09/2008. Fonte: Diário da Justiça - Data: 22/10/2008 - Página: 207 - Nº: 205 - Ano: 2008. Disponível em: <http://www.jusbrasil.com.br/jurisprudencia/8249976/apelacao-criminal-acr-5520-ce-0014586-4020054058100-trf5>. Acesso em: 29 de setembro de 2021.

_____. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Centro Gráfico, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html >. Acesso em: 29 de setembro de 2021.

CABRAL, Bruno Fontenele. **Breves comentários sobre a teoria da cegueira deliberada (willful blindness doctrine)**. Disponível em: <https://jus.com.br/artigos/21395/breves-comentarios-sobre-a-teoria-da-cegueira-deliberada-willful-blindness-doctrine> Acesso em: 29 de setembro de 2021.

CAMPOS, Fernando Teófilo. Sistemas de Common Law e de Civil Law: conceitos, diferenças e aplicações: Breves apontamentos sobre os Sistemas de

Common Law e de Civil Law. Disponível em:<https://jus.com.br/artigos/62799/sistemas-de-common-law-e-de-civil-law-conceitos-diferencas-e-aplicacoes> Acesso em: 29 de setembro de 2021.

CASTRO, Guilherme Fortes Monteiro de; GONÇALVES, Eduardo da Silva. **A aplicação da common Law no Brasil: diferenças e afinidades**. Disponível em: <http://www.ambito-juridico.com.br/site/?artigo_id=11647&n_link=revista_artigos_leitura> Acesso em: 29 de setembro de 2021.

COELHO, Edgard Lima. **A Intrínseca Relação entre o Crime de Lavagem de Dinheiro e as Organizações Criminosas.** Caderno de Pós-Graduação Caderno de Pós-graduação em Direito: Compliance e relações governamentais / coordenadores: Lilian Rose Lemos Rocha [et al.] – Brasília: UniCEUB: ICPD, 2019. Disponível em: <https://repositorio.uniceub.br/jspui/handle/prefix/13411> Acesso em: 29 de setembro de 2021.

ESTRELA, Kilmara Batista. **Crimes digitais**. 56f. (Trabalho de Conclusão de Curso - Monografia), Curso de Bacharelado em Ciências Jurídicas e Sociais – Direito, Centro de Ciências Jurídicas e Sociais, Universidade Federal de Campina Grande – Sousa- Paraíba - Brasil, 2003. Disponível em: <http://dspace.sti.ufcg.edu.br:8080/jspui/handle/riufcg/13373> Acesso em: 29 de setembro de 2021.

FREITAS, Rafael Sbeghen. **A Aplicabilidade da Teoria da "Cegueira" Deliberada ao Delito de Lavagem de Capitais no Brasil**. Disponível em: < https://repositorio.ufsc.br/bitstream/handle/123456789/193758/TCC%20RAFAEL%20S.%20FREITAS.pdf?sequence=1&isAllowed=y> Acesso em: 29 de setembro de 2021.

GRUPO ABRIL. **O avestruz enterra a cabeça quando fica com muito medo.** Disponível em: <https://super.abril.com.br/ciencia/o-avestruz-enterra-a-cabeca-quando-fica-com-muito-medo/> Acesso em: 29 de setembro de 2021.

LIMA, Milka Patrícia Vinhal de. A admissibilidade do dolo eventual e a aplicabilidade da cegueira deliberada no crime de lavagem de dinheiro: 2014. 54f. Monografia (Graduação) –Centro Universitário de Brasília, Brasília, 2014. Disponível em: http://www.repositorio.uniceub.br/handle/235/5996. Acesso em: 29 de setembro de 2021.

MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa**. Disponível em <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=teoria> Acesso em: 29 de setembro de 2021.

MONTEIRO, Taiana Alves. **Aplicação da Teoria da Cegueira Deliberada no Brasil**. Disponível em: <http://www.conjur.com.br/2009-set-28/necessario-dolo-especifico-caracterizacao-corrupcao-eleitoral>. Acesso em: 29 de setembro de 2021.

NASCIMENTO, André Ricardo Neto. **Teoria Da Cegueira Deliberada: Reflexos de sua aplicação à Lei de Lavagem de Capitais (Lei 9.613/98)**. Disponível em: <http://repositorio.uniceub.br/bitstream/123456789/800/1/20570516.pdf>. Acesso em: 29 de setembro de 2021.

PEREIRA, Ana Paula. **Facção criminosa utilizava Bitcoin para lavagem de dinheiro, afirma PM de São Paulo**. Disponível em: https://cointelegraph.com.br/news/criminals-used-bitcoin-for-money-laundering-says-sao-paulo-police. Acesso em: 29 set. 2021.

PEREIRA, Luiz Fernando. **O crime de lavagem de dinheiro e as moedas virtuais**. Disponível em: https://www.migalhas.com.br/depeso/298505/o-crime-de-lavagem-de-dinheiro-e-as-moedas-virtuais. Acesso em: 29 set. 2021.

PEREIRA, Mateus Henrique Chaves. A aplicabilidade da teoria da cegueira deliberada e o dolo eventual aos crimes de lavagem de dinheiro. 2018.54f. Monografia (Graduação) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2018. Disponível em: <https://repositorio.uniceub.br/jspui/handle/235/12570> Acesso em: 29 de setembro de 2021.

PEREIRA, Mateus Henrique Chaves. A aplicabilidade da teoria da cegueira deliberada e o dolo eventual aos crimes de lavagem de dinheiro. Acesso em: 29 de setembro de 2021.

REFLEXÕES SOBRE A CONSTITUCIONALIDADE DO ARTIGO 19 DO MARCO CIVIL DA INTERNET

Déborah Boechat Corrêa Lima [1]

RESUMO

Atualmente, a sociedade se encontra no auge da era da informação, em que as informações circulam numa velocidade nunca vista, em razão do desenvolvimento desenfreado da internet e da tecnologia. Como consequência da troca de informações acelerada, gerou-se uma falsa sensação de impunidade no ambiente virtual, de modo que parte dos usuários passou a utilizar as plataformas digitais como forma de agredir e ofender a imagem de outros, pelo que iniciou um significativo combate a essas ofensas ligado à necessidade de identificação e responsabilização do ofensor. Nesse contexto, foram aviadas insurgências por todo o país, mas dois recursos possuem destaque, pois foram reconhecidos pelo Supremo Tribunal Federal como temas de repercussão geral: RE nº 1.037.396/SP (Tema 987) e RE nº 1.057.258/MG (Tema 533). Ambos os Temas tratam do nível de responsabilidade dos provedores de internet diante da veiculação por meio das plataformas de conteúdos ilícitos gerados por terceiros, com a diferença de que o Tema 533 teve o seu debate iniciado antes da vigência do Marco Civil da Internet - Lei nº 12.965, de 23 de abril de 2014, e o Tema 987 aborda a análise da referida responsabilidade após o início da vigência do MCI, cujo resultado refletirá no reconhecimento da (in)constitucionalidade do artigo 19 do MCI. Assim, o presente estudo visa abordar os históricos processuais que deram origem a afetação dos Temas, bem como cotejar os princípios constitucionais e a legislação vigente em concomitância com o debate travado no bojo dos Temas 533 e 987 e da doutrina especializada no que tange à responsabilização dos provedores de aplicação da internet quanto à veiculação por meio da plataforma de conteúdos ilícitos gerados por terceiros.

Palavras-chave: Responsabilidade dos provedores de aplicação da internet. Conteúdos ilícitos. Temas 533 e 987 do STF.

ABSTRACT

Today society is at the height of the information age, in which information circulates at a speed never before seen, due to the unbridled development of the Internet and technology. As a consequence of this accelerated exchange of

[1] Aluna da pós-graduação *lato sensu* em Direito Digital.

information, a false sense of impunity was generated in the virtual environment, so that part of the users started to use the digital platforms as a way to attack and offend the images of others, so it began a significant fight against these offenses linked to the need for identification and accountability of the offender. In this context, insurgencies have been filed all over the country, and two appeals stand out, which were recognized by the Supreme Court as issues of general repercussion: RE No. 1,037,396/SP (Theme 987) and RE No. 1,057,258/MG (Theme 533). Both Themes deal with the level of responsibility of Internet providers in relation to the propagation of illicit content platforms by third parties, with the difference that Theme 533 had its debate started before the Civil Landmark of the Internet - Law No. 12,965 of April 23, 2014, and Theme 987 addresses the analysis of this responsibility after the beginning of the validity of MCI, whose result will reflect in the (in)constitutionality of Article 19 of MCI. Thus, this study aims to address the procedural background that gave rise to the assignment of the Themes, as well as to compare the legislation in force in concomitance with the debate held in the bulge of Themes 533 and 987 and the specialized doctrine regarding the liability of Internet application providers for the transmission through the platform of illegal content generated by third parties.

Keywords: Responsibility of internet application providers. Illegal content. Themes 533 and 987 of STF.

1 INTRODUÇÃO

O uso massivo das redes sociais transformou a forma como as pessoas se expressam, porquanto as redes concentram grande parte das manifestações de pensamento em todo o mundo. Entretanto, se por um lado as mídias digitais proporcionam facilidade de comunicação a nível mundial, o uso das redes também expõe a sociedade a riscos de violações a direitos fundamentais, pois a sociedade manifesta suas opiniões e pensamentos “protegida” por uma tela de computador levada por uma sensação de anonimato. Dessa forma, considerando a acelerada promoção das redes sociais como principal meio de comunicação e fonte de informação, a mesma sociedade que as usa desenfreadamente começou a demandar tanto dos provedores de internet quanto do Estado uma posição mais enérgica quanto aos ilícitos cometidos por meio das plataformas.

Os mecanismos de identificação, suspensão e banimento de usuários e robôs que impulsionam e disparam mensagens em massa estão em constante discussão desde as eleições gerais de 2018, quando esse recurso – o envio em massa de notícias falsas por aplicativos de mensagens, e das mídias digitais no geral - tornou-se um fenômeno de propagação usual entre candidatos e partidos políticos.

E sempre que há novas ferramentas, especialmente tecnológicas, surgem novos questionamentos filosóficos, sociais e jurídicos envolvendo os impactos que elas reproduzem na sociedade. Não haveria de ser diferente quanto aos limites do direito à liberdade de expressão e da responsabilização civil dos provedores de internet no Brasil.

No contexto brasileiro, os principais eixos que vem conduzindo as discussões sobre regulação de intermediários estão no Marco Civil da Internet (MCI), Lei nº. 12.965/2014, nos artigos 9, que trata da neutralidade da rede, e 19, que estabeleceu um modelo de isenção de responsabilidade civil parcial voltada a intermediários de internet por conteúdos que não sejam de sua autoria.

O debate a respeito desse modelo de responsabilização deflagrou a interposição de vários recursos pelo País, dentre eles, destacam-se dois, que foram reconhecidos pelo Supremo como temas de repercussão geral: RE nº 1.037.396/SP (Tema 987) e RE nº 1.057.258/MG (Tema 533).

Serão abordados, nesse trabalho, os históricos processuais desses recursos e a discussão sobre os Temas, no que tange à remoção e responsabilização dos provedores de aplicação da internet quanto a conteúdos ilícitos gerados por terceiros por intermédio das plataformas, e como a segurança jurídica fornecida pelo art. 19 aponta um equilíbrio entre as de liberdades constitucionais de informação e de expressão.

2 O HISTÓRICO PROCESSUAL DOS TEMAS 533 E 987 DO STF

Em dezembro de 2019, o STF havia convocado audiência pública para o dia 23 de março de 2020, com intuito de ouvir o depoimento de autoridades e especialistas sobre i) o regime de responsabilidade de provedores de aplicativos ou de ferramentas de internet por conteúdo gerado pelos usuários, e ii) a possibilidade de remoção de conteúdos que possam ofender direitos da personalidade, incitar o ódio ou difundir notícias fraudulentas a partir de notificação extrajudicial.

Tendo em vista o disposto na Resolução STF nº 663, de 12 de março de 2020, que estabeleceu medidas temporárias de prevenção ao contágio pelo COVID-19,

restou suspensa a audiência pública convocada, a qual trataria dos Temas 533 e 987 da gestão por temas da sistemática da repercussão geral, nos âmbitos do RE nº 1.037.396/SP e do RE nº 1.057.258/MG. Segundo o Tribunal, novas datas serão designadas oportunamente e divulgadas.

O Tema 533 versa sobre o dever de empresa hospedeira de sítio na internet de fiscalizar o conteúdo publicado e de retirá-lo do ar, sem intervenção judicial, quando ele for considerado ofensivo. Por sua vez, o Tema 987 revela discussão sobre a constitucionalidade do art. 19 do MCI, que torna necessária a existência de prévia e específica ordem judicial de remoção de conteúdo para que, em caso de descumprimento da ordem, haja a responsabilização civil de provedores de internet, hospedeiros de websites e gestores de aplicativos de redes sociais por danos decorrentes de conteúdos ilícitos veiculados por terceiros.

2.1 O Tema 533 (Recurso Extraordinário nº 1.057.258/MG)

O Recurso Extraordinário nº 1.057.258/MG, cujo Relator é o Ministro Luiz Fux, foi interposto pela empresa Google Brasil Internet Ltda. contra acórdão proferido pela Primeira Turma Recursal de Belo Horizonte/MG.

Na origem, trata-se de ação ajuizada em 18 de janeiro de 2010 por Aliandra Cleide Vieira, professora de ensino médio, contra o Google em razão da suposta criação de um grupo/comunidade denominada “Eu odeio a Aliandra” na antiga rede de relacionamento Orkut, que pertencia ao Google.

Segundo a autora, o grupo foi criado por seus alunos com o objetivo de veicular ofensas à sua personalidade e dignidade, inclusive com a postagem de fotos da professora contendo alegações de injúria, o que teria lhe causado prejuízos de ordem emocional, constrangimento e vergonha perante sua família, amigos, alunos e colegas de profissão. Ela solicitou ao Google, por meio de carta registrada, que retirasse do ar a comunidade do Orkut, porém a empresa teria negado a remoção em razão da ausência de verificação de violação das “*leis do mundo real”* ou das políticas da plataforma.

O pedido de indenização dos danos morais foi pautado nos direitos à imagem e à honra, dispostos no art. 5º, V, da Constituição Federal (CF)[2], assim como o direito à intimidade, à vida privada e o direito a obter indenização pelo dano material ou moral decorrente de sua violação[3], considerando o fato de que "a proteção jurídica à imagem da pessoa é fundamental para a manutenção da sociedade segura e harmônica, pois a honra subjetiva e objetiva do cidadão são direitos indispensáveis à boa convivência com os seus semelhantes e consigo próprio".

Para a professora, uma vez que a empresa não exerce nenhum controle sobre o conteúdo veiculado por terceiros na rede social, o que a leva a assumir a responsabilidade por sua omissão voluntária ao permitir a prática de atos ilícitos em seu domínio, havendo de ser responsabilizada por sua conivência, uma vez que seria do ofendido a conclusão acerca da necessidade de retirada ou não do conteúdo agressivo da internet.

Na sentença, que julgou procedente a demanda, restou consignado que a empresa teria incorrido em omissão ao não adotar providências com o fito de impedir "o uso da imagem da autora de forma não autorizada por ela, e mais, impediria que ela continuasse a ser ridicularizada na comunidade escolar, especialmente, dentre o corpo discente", ainda que tenha sido notificada extrajudicialmente para proceder com a remoção do conteúdo ofensivo.

O Google interpôs recurso inominado e noticiou o cumprimento da ordem, alegando que a sua responsabilidade é subjetiva, considerando que sua atividade não se caracteriza como de risco, não existindo dever de indenizar por parte da empresa que, apesar de informada sobre o conteúdo postado, não identificou, em sua análise, violação dos termos e políticas estabelecidos pelo site, sendo necessário pronunciamento judicial para a remoção do referido conteúdo.

O acórdão proferido pela 1ª Turma Recursal Cível do TJMG consignou que "a recorrente foi informada pela recorrida sobre as manifestações publicadas na

[2] Art. 5º […] V – é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem; […].

[3] Art. 5º […] 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; […].

página e que se sentia ofendida com o conteúdo, mesmo assim permitiu que as publicações continuassem disponíveis para acesso pelos usuários".

Logo, a condenação da empresa veio amparada, não só na ausência de fiscalização do Orkut, como numa suposta negligência da empresa, pois não teria removido o conteúdo imputado danoso após provocação da recorrida.

Por essa lógica, o Google supostamente deveria ser responsabilizado por não fiscalizar todo e qualquer tipo de conteúdo postado pelos usuários do Orkut, o que, de pronto, seria vedado pela CF, pois poderia implicar em censura prévia, em afronta aos arts. 5º, IV, IX, XIV, XXXIII e 220, §§ 1º, 2º e 6º da CF[4]. Por outro lado, sendo exigível do Google a remoção de conteúdos no âmbito extrajudicial, poderia implicar em violação à reserva de jurisdição do Poder Judiciário, previsto no art. 5º, XXXV da CF[5], pois a empresa privada teria de exercer juízo de valor sobre os conteúdos altamente subjetivos de terceiros e ponderar garantias constitucionais.

Após a oposição de embargos de declaração, que não foram acolhidos, o Google interpôs recurso extraordinário alegando (i) a violação do direito à livre manifestação do pensamento e à vedação à censura, previsto nos arts. 5º, II, IV, IX, XIV, XXXIII, e 220, §§1º, 2º e 6º, todos da CF, o que impossibilitaria a fiscalização prévia, o monitoramento e a varredura de conteúdo, posto que configuraria censura prévia praticada por empresa privada; (ii) dificuldade de avaliação de eventual lesão a direito de usuários e terceiros, oriunda da subjetividade das informações

[4] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] IV - é livre a manifestação do pensamento, sendo vedado o anonimato; [...] IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; [...] XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; [...] XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição. § 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV. § 2º É vedada toda e qualquer censura de natureza política, ideológica e artística. [...] § 6º A publicação de veículo impresso de comunicação independe de licença de autoridade.

[5] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] XXXV - a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito;

armazenadas pelos usuários, tais como sátiras, críticas e deboches, constituindo-se em conduta arbitrária a avaliação e a retirada unilateral dos dados pelo próprio Orkut; (iii) a necessidade de intervenção do Poder Judiciário sobre os litígios de igual natureza, pois é o único legitimado a avaliar eventual ofensa a direitos decorrentes de manifestações armazenadas em sítios de relacionamento e (iv) a inexistência de graves ofensas na comunidade excluída e que a professora, em sua notificação extrajudicial, não explicitou nenhuma razão que justificasse a interferência do Google no caso analisado.

Inadmitido o Extraordinário, a recorrente interpôs agravo e os autos foram remetidos ao Supremo Tribunal Federal (STF). O agravo foi distribuído ao Ministro Luiz Fux e autuado sob o Recurso Extraordinário com Agravo (ARE) nº 660861. O Supremo reconheceu, por maioria[6], a existência de repercussão geral da questão constitucional suscitada, pelo que foi determinada vista do feito à Procuradoria-Geral da República (PGR) e se manifestou pelo desprovimento do recurso.

Diante da indicação da repercussão geral, após parecer ministerial, houve novo encaminhamento dos autos à PGR para manifestação sobre a entrada em vigor do MCI, oportunidade em que a PGR concordou com a substituição do paradigma. Então, o ARE nº 660861 foi autuado como Recurso Extraordinário nº 1057258 e se tornou o paradigma da repercussão geral do Tema 533 – Dever de empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário.

Em manifestação avulsa, o Google aduziu que a questão constitucional deixou de existir em razão do voto do Ministro Relator, o qual, na análise da repercussão da matéria, indicou a ausência de regulamentação legal, sob o seguinte argumento:

> Insta definir, à míngua de regulamentação legal da matéria, se a incidência direta dos princípios constitucionais gera, para a empresa hospedeira de sítios na rede mundial de computadores, o dever de fiscalizar o conteúdo publicado nos seus domínios eletrônicos e de retirar do ar as informações reputadas ofensivas, sem necessidade de intervenção do Judiciário. Considero que a matéria possui Repercussão Geral,

[6] Vencido o Ministro Marco Aurélio. Não se manifestaram os Ministros Gilmar Mendes, Joaquim Barbosa, Cármen Lúcia e Rosa Weber. 23/03/2012 - Plenário Virtual – RG.

> apta a atingir inúmeros casos submetidos à apreciação do Poder Judiciário.

Para o Google, com a entrada em vigor do MCI, a lacuna legal foi superada e, consequentemente, houve a perda superveniente de objeto. A recorrida se manifestou contrária a essa alegação e requereu o prosseguimento do feito.

Ademais, a empresa alega que o art. 21 do MCI[7], que trata dos casos de remoção de conteúdo em casos contendo nudez ou conteúdo sexual de caráter privado, não abarcou outros casos que extensivamente devem ser apreciados pelo Poder Judiciário.

Em petição avulsa, o Google requereu, em novembro de 2019, o julgamento conjunto do RE nº 1.057.258/MG com o RE nº 1.037.396/SP, que teve a repercussão geral reconhecida pelo Plenário Virtual do STF (Tema 987), de modo a permitir o exame completo das questões jurídicas em análise.

Apesar da entrada em vigor do MCI, o STF consignou que não seria cabível falar na aplicação do art.19 do MCI ao caso da professora, ocorrido em 2010, em razão do princípio da irretroatividade legal, bem como que a discussão posta no presente caso continuaria a ostentar caráter constitucional e possuir repercussão geral.

2.2 O Tema 987 (Recurso Extraordinário nº 1.037.396/SP)

Em trâmite perante o STF, o Recurso Extraordinário nº 1.037.396/SP, autuado em 2017 e distribuído à relatoria do Ministro Dias Toffoli, foi interposto pelo Facebook em face de acórdão proferido pela 2ª Turma Recursal Cível do Colégio Recursal de Piracicaba/SP que, declarando incidentalmente a inconstitucionalidade do art. 19 do MCI, condenou a empresa ao pagamento de indenização por danos morais em razão da omissão, mesmo após provocação extrajudicial, para excluir de sua plataforma virtual suposto perfil falso criado em nome de terceira pessoa.

[7] Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Na origem, trata-se de ação de obrigação de fazer e pedido de indenização por danos morais ajuizada por Lourdes Pavioto Corrêa contra a rede social, objetivando a exclusão de perfil falso da plataforma e o fornecimento de dados de IP (internet protocol) do computador utilizado para a criação do perfil falso, pretendendo a reparação pelos prejuízos causados à sua honra e imagem pelo conteúdo das publicações feitas em seu nome.

Após a determinação de remoção do perfil em caráter liminar, a demanda foi julgada parcialmente procedente para confirmar os efeitos da antecipação de tutela, bem como para ordenar que o Facebook apresentasse, em 10 dias, o número do IP utilizado para a criação da referida página. Todavia, quanto ao pedido de pagamento de danos morais, o magistrado considerou inexistir ato ilícito a ensejá-los, sob o fundamento de que a conduta da rede social, ao aguardar pronunciamento jurisdicional para promover a exclusão do perfil falso, encontrou respaldo no disposto no art. 19 do MCI.

Tanto a autora quanto o Facebook interpuseram recursos inominados, os quais foram acolhidos pela 2ª Turma Recursal Cível do Colégio Recursal de Piracicaba/SP, para condenar o Facebook Brasil ao pagamento de indenização no valor de R$ 10.000,00 e para eximi-lo do fornecimento do IP.

De acordo com a decisão recorrida, em vista do preceito constitucional da defesa do consumidor, previsto no art. 5º, inciso XXXII[8], o art. 19 do MCI seria inconstitucional, prevalecendo a responsabilidade objetiva do fornecedor de serviços prevista no art. 14 do Código de Defesa do Consumidor[9].

Em face do acórdão foram opostos embargos de declaração, os quais restaram rejeitados, pelo que o Facebook interpôs o Recurso Extraordinário, no qual defende a repercussão geral da questão, indicando a existência de similitude com a matéria debatida no RE nº 1.057.258/ MG, paradigma do Tema 533 da Repercussão Geral.

[8] XXXII - o Estado promoverá, na forma da lei, a defesa do consumidor.

[9] Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

No mérito, sustenta a constitucionalidade do art. 19 do MCI, afirmando sua compatibilidade com o disposto no art. 5º, incisos IV[10], IX[11], X[12], XIV[13], XXXV[14] e art. 220, caput[15] e § 2º[16], da CF. Nesse sentido, defende que impor a empresas privadas provedoras de aplicações de internet a obrigação de fiscalizar e excluir conteúdo gerado por terceiros, sem prévia apreciação do Poder Judiciário, configura risco de censura e restrição à liberdade de manifestação dos usuários da rede mundial de computadores.

Houve a determinação de sobrestamento do feito para aguardar pronunciamento definitivo do STF quanto ao Tema 533, mas a empresa pleiteou pelo prosseguimento sob argumento de que o recurso extraordinário por ela interposto é debatido à luz da disciplina inaugurada pelo MCI, a qual ainda não havia sido promulgada quando da indicação da repercussão geral do Tema 533, o que foi acolhido.

Autuado o recurso, o Plenário, por maioria[17], reconheceu a existência de repercussão geral da questão constitucional suscitada no apelo (01/03/2018), escolhendo-o como paradigma do Tema 987, que foi assim delimitado[18]:

> 987 - Discussão sobre a constitucionalidade do art. 19 da Lei n. 12.965/2014 (Marco Civil da Internet) que determina a necessidade de prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, websites e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros.

O artigo 19 do MCI está assim disposto:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet

[10] IV - é livre a manifestação do pensamento, sendo vedado o anonimato.
[11] IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença.
[12] 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.
[13] XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional.
[14] XXXV - a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito.
[15] Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
[16] § 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.
[17] Vencido o Ministro Edson Fachin. Não se manifestou a Ministra Cármen Lúcia.
[18] Disponível em: http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5160549&numeroProcesso=1037396&classeProcesso=RE&numeroTema=987.

> 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.

O que se discute, nesse caso, é a opção do legislador quanto ao regime de responsabilização civil dos provedores de aplicações de internet por conteúdos criados por terceiros, usuários das aplicações.

E, através da decisão de afetação, definiram-se os questionamentos que deverão ser respondidos quando do julgamento da demanda, quais sejam: se o provedor de aplicação da internet (i) deve proceder com a fiscalização do conteúdo veiculado por meio de suas plataformas, (ii) deve remover as informações reputadas ofensivas mediante simples notificação extrajudicial, (iii) deve ser responsabilizado legalmente pela veiculação do conteúdo antes da análise do Poder Judiciário.

A partir dos históricos traçados, vê-se que os Temas possuem identidade, que é a responsabilização de provedores de aplicações e o pano de fundo da discussão são os limites e riscos à liberdade de expressão; o que difere os dois recursos é o fato deste último se referir à discussão da matéria antes da promulgação do MCI.

3 AS LIBERDADES CONSTITUCIONAIS DE INFORMAÇÃO E DE EXPRESSÃO

A Constituição de 88 trouxe extenso rol de direitos concernentes à proteção da liberdade: liberdade de pensamento, de expressão, religiosa e de culto, ideológica e de reunião, bem como a liberdade de imprensa, também essencial para a sobrevivência de democracias, sendo vedada toda e qualquer espécie de censura ou licença.

A liberdade de expressão e de informação é um direito reconhecido internacionalmente, em tratados e declarações de organismos multilaterais. Estão fundamentadas de forma conjunta no artigo 19 da Declaração Universal dos Direitos Humanos, de 10 de dezembro de 1949:

> "Todo ser humano 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".

As liberdades de expressão e de livre manifestação de pensamento e o direito à informação, para além de serem garantias constitucionais individuais, também traduzem um direito de dimensão coletiva, no sentido de permitir que a sociedade como um todo se manifeste e se informe. Quando positivadas em normas constitucionais, como ocorre no Brasil, elas podem ser invocadas independentemente de o legislador colocar previsões nesse sentido, dado o poder vinculador das normas constitucionais[19].

A esse respeito, Barroso leciona que as liberdades de informação e de expressão, tanto em sua manifestação individual, como na coletiva, servem de fundamento para o exercício de outras liberdades, o que justifica uma posição de preferência em relação aos direitos fundamentais individuais considerados, a qual "deve resultar a absoluta excepcionalidade da proibição prévia de publicações, reservando-se essa medida aos raros casos em que não seja possível a composição posterior do dano que eventualmente seja causado aos direitos da personalidade"[20].

A doutrina distingue as liberdades de informação e de expressão, a primeira diz respeito ao direito individual de comunicar livremente fatos e ao direito difuso de ser deles informado e a segunda destina-se a tutelar o direito de externar qualquer manifestação do pensamento humano. Para Barroso, não há dúvidas de que "a liberdade de informação se insere na liberdade de expressão em sentido amplo, mas a distinção parece útil por conta de um inegável interesse prático, relacionado com os diferentes requisitos exigíveis de cada uma das modalidades e suas possíveis limitações" [21].

A informação não pode abstrair a verdade, pela circunstância de que é isso que as pessoas supõem estar conhecendo ao buscá-la, requisito que não está presente

---

[19] CANOTILHO, José Joaquim Gomes; MACHADO, Jónatas E. M.; JÚNIOR, Antônio Pereira Gaio. **Biografia não autorizada versus liberdade de expressão**. Curitiba: Juruá Editora, 2014. p. 27-28.

[20] BARROSO, Luís Roberto. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. **Revista de Direito Administrativo,** Rio de Janeiro, v. 235: 1-6, jan. 2004. p. 20. Disponível em: https://doi.org/10.12660/rda.v235.2004.45123.

[21] BARROSO, Luís Roberto. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. **Revista de Direito Administrativo,** Rio de Janeiro, v. 235: 1-6, jan. 2004. p. 18. Disponível em: https://doi.org/10.12660/rda.v235.2004.45123.

nas manifestações da liberdade de expressão. Logo, haverá o exercício do direito de informação quando a finalidade da manifestação for a comunicação de fatos noticiáveis, cuja caracterização repousa no critério da sua verdade[22].

Para Cláudio Luiz Bueno de Godoy, "a liberdade de informação, em lato senso, compreende tanto a aquisição como a comunicação de conhecimentos"[23], pois compreende o direito de estar informado (direito à informação) e o direito de ter e compartilhar informação (direito à comunicação).

O direito à liberdade de expressão, direito fundamental assegurado pela CF, tem como principal intuito garantir a dignidade da pessoa humana por meio da livre expressão de ideias, opiniões e pensamentos. A liberdade de expressão traduz-se na faceta externa da liberdade de pensamento, conferindo a Constituição uma tutela em caráter genérico para a manifestação do pensamento.

Desse modo, a liberdade de expressão é um direito inerente à pessoa humana e possui um conceito amplo que consiste na exteriorização do pensamento, de ideias, opiniões, convicções, sensações e sentimentos através de atividades intelectuais, artísticas, científicas ou por qualquer outra forma de se comunicar, o qual cabe ao Estado não apenas reconhecer o direito à liberdade, mas incentivá-lo e tutelá-lo[24].

A tutela conferida à liberdade de expressão e de informação, está prevista no art. 5º, inciso IV, da CF, que garante a livre manifestação do pensamento, sendo vedado o anonimato, e no art. 5º, XIV, segundo o qual "é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional".

Para tratar dos meios de comunicação social e da liberdade de imprensa, o art. 220 da CF, estabelece que "A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição".

---

[22] BARROSO, Luís Roberto. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. **Revista de Direito Administrativo**, Rio de Janeiro, v. 235: 1-6, jan. 2004. p. 18-19. Disponível em: https://doi.org/10.12660/rda.v235.2004.45123.

[23] GODOY, Cláudio Luiz Bueno de. **A liberdade de imprensa e os direitos da personalidade**. 2. ed. São Paulo: Atlas, 2008.

[24] MEYER-PFLUG, Samantha Ribeiro. **Liberdade de expressão e discurso do ódio**. São Paulo: Editora Revista dos Tribunais, 2009. p.66.

Assim, ao oferecer um ambiente favorável ao desenvolvimento da liberdade de expressão, o texto constitucional busca criar condições para o desenvolvimento da democracia.

3.1 Colisão dos direitos fundamentais

Segundo Manuela Cibim Kallajian, "Basta uma pesquisa singela para se apurar que não há uma única forma de solução para o impasse aqui apresentado e isso ocorre justamente porque a resposta dependerá da formação do sistema pelo intérprete"[25].

Para Maria Helena Diniz, a hermenêutica jurídica contém regras que fixam os critérios e princípios que deverão nortear a interpretação, contudo é preciso compreender a norma em atenção aos seus fins sociais e aos valores que pretende garantir, "pois o intérprete deve levar em conta o coeficiente axiológico e social nela contido, baseado no momento histórico em que está vivendo"[26].

À vista disso, há quem sustente que o § 1º do art. 220, da CF, ao afirmar que "Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV", restringe a ponderação ao julgamento dos casos concretos, afastando a possibilidade de o legislador a realizar em abstrato.

Segundo seus defensores, os direitos da personalidade são direitos fundamentais previstos na CF, cujas normas devem ser interpretadas de maneira sistemática, de modo a evitar contradições entre si. Nesse sentido, leciona Manuela Cibim Kallajian:

> [...] processo sistemático, ou como prefere Vicente Ráo, processo lógico-sistemático que "em nada mais consiste senão no processo comparativo ensinado pela lógica e revestido de certas peculiaridades próprias das ciências jurídicas". Como unidade, o sistema não pode ser encarado como um aglomerado aleatório de disposições legais, pois não se pode entender integralmente uma coisa sem entender suas partes, da

[25] KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão**: conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 184.
[26] DINIZ, Maria Helena. **Compêndio de introdução à ciência do direito.** 24. ed. São Paulo: Saraiva, 2013. pp. 441 e 451.

> mesma forma que não se pode compreender as partes de alguma coisa sem a compreensão do todo.[27]

Utilizando o processo lógico-sistemático, o texto constitucional deve ser encarado como uma unidade e um sistema em que não pode haver incoerências. E, ao menos na questão do caso, não há, pois o art. 220 da CF determina que "A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição" e o seu § 1º estabelece que "Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV".

Assim, a própria CF afirma, embora voltada para veículos de comunicação social, que a liberdade de expressão e a informação devem observar o direito à vida privada. Para Manuela Cibim Kallajian, seria dizer que "o direito à privacidade é limite à liberdade de expressão e informação"[28].

Portanto, para essa corrente, ao analisar os dispositivos constitucionais em conjunto, vislumbra-se que a própria Constituição aponta para a solução do conflito, dando a diretriz ao intérprete. Assim, o conflito não se trata de uma antinomia real, e sim de um aparente conflito de normas, restando ao intérprete buscar a conciliação possível entre as proposições aparentemente antagônicas[29].

A importância da interpretação lógico-sistemática da CF, juntamente com o princípio da unidade, se dá porque nos força a interpretar o texto constitucional a fim de evitar contradições.

Maria Helena Diniz aponta solução diversa, para a autora, havendo conflito entre direitos da personalidade, que também são direitos fundamentais, se estaria diante de

> [...] uma antinomia real ou lacuna de colisão, por não haver na ordem jurídica qualquer critério normativo para solução, a não

[27] KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão**: conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 184.
[28] KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão:** conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 195.
[29] KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão:** conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 195-196.

> ser pela edição de uma nova norma que escolha uma das normas conflitantes, ou pelo emprego da interpretação corretivo-equitativa, refazendo o caminho da fórmula normativa, tendo presente fatos e valores, para aplicar significado objetivado pelas normas conflitantes.[30]

Independentemente das teses que se acaba de registrar, a liberdade de informação e de expressão, não são direitos absolutos, encontrando limites na própria Constituição. Assim, apesar de a CF/88 conferir amplo tratamento ao tema da liberdade de pensamento e de expressão, garantido a qualquer pessoa expressar o que pensa ou sente, estabelecendo que "é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença", essa liberdade não é ilimitada, pois vem conformada pela licitude da manifestação e a observância de outras normas jurídicas e princípios constitucionais, não ficando imune à responsabilidade por eventual dano causado a terceiros.

Um dos limites da liberdade de expressão está no inciso X do art. 5º, da CF, que explicita a proteção da incolumidade física e moral da pessoa humana ou jurídica, ao estabelecer que "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". Outro limite à liberdade de expressão estaria na concepção da verdade, especialmente quando se trata da liberdade de imprensa, pois conduziria a uma pseudo-operação da formação da opinião[31].

Há, ainda, um limite genérico às liberdades de informação e de expressão que consiste no interesse público, o qual compreende o conteúdo veiculado pelo agente, logo procura-se fazer um juízo de valor sobre o interesse na divulgação de determinada informação ou opinião[32]. Nesse contexto, Barroso afirma que há um interesse público na própria liberdade, independente do conteúdo, tendo em vista que é sobre essa liberdade que se deve construir a confiança nas instituições e na democracia, pois "O Estado que censura o programa televiso de má qualidade pode,

---

[30] DINIZ, Maria Helena. Efetividade do direito a ser esquecido. **Revista Argumentum,** v. 18, n. 1, p.24, jan./abr. 2017. Disponível em: http://ojs.unimar.br/index.php/revistaargumentum/article/view/339.

[31] BRANCO, Paulo Gustavo Gonet. Direitos Fundamentais em Espécie. In: MENDES, Gilmar Ferreira. **Curso de Direito Constitucional.** 9. ed. São Paulo: Saraiva, 2014.

[32] BARROSO, Luís Roberto. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. **Revista de Direito Administrativo**, Rio de Janeiro, v. 235: 1-6, jan. 2004. p. 24. Disponível em: https://doi.org/10.12660/rda.v235.2004.45123.

com o mesmo instrumental, censurar matérias jornalísticas "inconvenientes", sem que o público exerça qualquer controle sobre o filtro que lhe é imposto" [33]. Portanto, pode se concluir que o interesse público na divulgação de informações é presumido.

Somente no caso concreto é que se poderá analisar se houve excesso no exercício do direito de expressar ou de informar que tenha violado a esfera íntima do indivíduo, posto que são fortemente assegurados os direitos à livre manifestação do pensamento e de expressão, bem como o direito de informar e ser informado, desde que não se ultrapasse o limite da liberdade alheia[34].

Assim, em que pese a própria Constituição tenha dado orientação de que a liberdade de expressão e a informação devem observar o direito à privacidade, o caso concreto pode conter nuances que exijam do julgador uma interpretação específica e esta não é e não pode ser uma aplicação literal ou neutra da norma positivada, tendo em vista que não se poderá excluir uma das normas em benefício de outra.

Protegidos constitucionalmente como direitos fundamentais, intimidade, liberdade de expressão e de informação não possuem hierarquia entre si, por força do princípio da unidade da Constituição, não havendo a possibilidade de eleger uma única premissa a ser aplicada.

Segundo Manuela Kallajian, "A colisão entre princípios constitucionais decorre do pluralismo, da diversidade de valores e interesses que se abrigam no documento dialético e compromissário que é a Constituição"[35]. A colisão de princípios constitucionais ou de direitos fundamentais não se resolve mediante o emprego dos critérios tradicionais de solução de conflitos de normas, como o hierárquico, o temporal e o da especialização.

Dessa maneira, frente à colisão entre direitos fundamentais, imagem e honra de um lado e liberdade de informação e de expressão do outro, deve ser aplicado o

[33] BARROSO, Luís Roberto. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. **Revista de Direito Administrativo**, Rio de Janeiro, v. 235: 1-6, jan. 2004. p. 24. Disponível em: https://doi.org/10.12660/rda.v235.2004.45123.

[34] KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão:** conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 196.

[35] KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão:** conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 200.

princípio da proporcionalidade no caso concreto, por meio do qual se operacionaliza o método da ponderação prestigiando-se os direitos que, nas circunstâncias valoradas, ostentem maior interesse público e social[36].

A ponderação deverá decidir não apenas qual bem constitucional deve preponderar no caso concreto, mas também em que medida ou intensidade ele deve preponderar. A restrição mais radical seria a proibição prévia da publicação ou divulgação do fato ou da opinião, pois essa modalidade de restrição elimina a liberdade de informação e de expressão. Em seguida, a própria Constituição admite a existência de crimes de opinião e a responsabilização civil por danos materiais ou morais.]

4 REFLEXÕES SOBRE OS TEMAS E AS SUAS SIMILITUDES

No RE do Tema 533, o Google argumenta que, com a edição do MCI, em princípio, teria ocorrido o esvaziamento da repercussão geral discutida no *leading case*. No entanto, o STF sinalizou que, apesar da entrada em vigor da norma, a discussão posta no caso paradigma continuaria a ostentar caráter constitucional e possuir repercussão geral. Com efeito, ao se manifestar pelo reconhecimento de repercussão geral no novo paradigma (posterior ao MCI), o Ministro Dias Toffoli indicou a necessidade de que o novo recurso seja apreciado em paralelo ao Tema 987 - Recurso Extraordinário nº 1.037.396/SP, justamente para que o STF analise o tema de forma completa.

Registra-se que os fatos que deram origem à discussão do Tema 533 datam dos anos de 2009 e 2010, período anterior à edição da Lei 12.965/2014. O Tema 987, por sua vez, engloba a discussão sobre a constitucionalidade do art. 19 do MCI que determina a necessidade de prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, *websites* e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros.

[36] KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão:** conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 197.

Assim, ambos recursos tratam de tema comum – a responsabilização de provedores de serviços, sendo que um deles tem regramento estabelecido por lei específica e o outro não.

No período anterior ao MCI, não existia jurisprudência uniforme sobre a responsabilidade dos provedores de aplicação da internet, que estava sujeita a uma série de interpretações distintas. À época, o entendimento dominante era no sentido de reconhecer a responsabilidade do provedor de aplicação que deixava de adotar as providências para a remoção do conteúdo ilícito após o recebimento de notificação extrajudicial, não sendo necessária uma ordem judicial nesse sentido, ou seja, o sistema de notificação e retirada ("*notice and takedown*").

Com a entrada em vigor da lei, que estabelece a regra para responsabilização dos provedores de aplicações de internet, esperava-se que a tese debatida estaria pacificada. Porém, o entendimento sobre o papel dos provedores de aplicação da internet quanto a conteúdos considerados ilícitos veiculados por terceiros, como já demonstrado, ainda padece de solução definitiva. E, para amparar o debate, imprescindível se faz estabelecer alguns conceitos.

Ambos os temas tratados neste artigo refletem colisões que necessitam de observação, o Tema 533 aborda a colisão entre direitos fundamentais, enquanto o Tema 987 trata da colisão entre legislações federais.

A fim de solucionar o aparente conflito entre normas e direitos, Manuela Kallajian afirma que, primeiramente, o julgador deve detectar no sistema as normas que estão em conflito e agrupá-las em função da solução que estejam sugerindo, feito isto, o intérprete deve passar a examinar os fatos e sua interação com os elementos de ponderação e "Só então o intérprete poderá sopesar os elementos em disputa, indicando qual deve prosperar" [37]. Todo esse processo intelectual tem como fio condutor o princípio da proporcionalidade.

[37] KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão**: conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 205.

4.1 A colisão entre direitos fundamentos e o Tema 533

Como mencionado, o Tema 533 reflete a colisão entre direitos fundamentais, imagem e honra de um lado e liberdade de informação e de expressão do outro.

Sobre o tema, Barroso entende que diante da colisão a liberdade de expressão e informação, de um lado, e os direitos à honra, à intimidade, à vida privada e à imagem, de outro, destacam-se como elementos de ponderação a veracidade do fato, licitude do meio empregado na obtenção da informação, personalidade pública ou estritamente privada da pessoa objeto da notícia, local do fato, natureza do fato, existência de interesse público na divulgação em tese, existência interesse público na divulgação de fatos relacionados com a atuação de órgãos públicos e preferência por sanções a posteriori, que não envolvam a proibição prévia da divulgação.

Já para Manuela Kallajian, o critério mais e importante e o primeiro que deve ser pesado é o de interesse público, no qual "Somente se autoriza a divulgação de fatos relativos à privacidade de um indivíduo quando se evidencia algo justificador da intromissão que, por seu objeto ou valor, revele matéria merecedora de difusão" [38].

Outro elemento importante é o da veracidade da informação, porque, não sendo a informação verdadeira, não há razão para seu crédito e muito menos para sua divulgação[39]. A informação que goza de proteção constitucional é a informação verdade. A divulgação deliberada de uma notícia falsa, em detrimento do direito da personalidade de outrem, não constitui direito fundamental do emissor[40].

O conflito entre privacidade e liberdade de expressão deverá ser solucionado com a observância particular do princípio da dignidade humana. A esse respeito, leciona Manuela Kallajian:

> Para o balanceamento dos direitos em conflito através dos critérios acima propostos, deverá existir uma diretriz mestra

[38] KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão**: conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 203.

[39] KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão**: conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 204.

[40] BARROSO, Luís Roberto. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. **Revista de Direito Administrativo**, Rio de Janeiro, v. 235: 1-6, jan. 2004. Disponível em: https://doi.org/10.12660/rda.v235.2004.45123.

> que dirigirá o intérprete. [...] Esse comando se chama dignidade da pessoa humana. [...] Não se pode falar em vida digna sem o respeito à parte íntima, secreta e profunda do ser humano. Também não se pode falar em dignidade quando se é impedido de expressar livremente seu pensamento e opinião. Mas há de se analisar que o ordenamento constitucional não agasalha violências ou arbitrariedades, servindo o princípio da dignidade da pessoa humana como termômetro para a mensuração e aferição de abusos, sem com vistas ao saudável desenvolvimento da personalidade humana.[41]

Tais parâmetros servem de guia para o intérprete no exame das circunstâncias do caso concreto e permitem certa objetividade às suas escolhas.

Caso houvesse um dever de remoção automática, os provedores de redes sociais seriam obrigados a remover a crítica a pedido do criticado e todas as manifestações produzidas na rede correriam o risco de ser suprimidas e a internet perderia todo o seu potencial de canal de informação, inviabilizando de forma drástica a liberdade de informação ou de expressão.

Considerando a impossibilidade física de tal providência, bastaria o indivíduo que está sendo alvo de críticas negar a suposta autorização e assim tornar possível ao provedor de redes sociais desempenhar o seu papel institucional.

No caso, portanto, o critério de ponderação deve ser a análise da atitude do suposto ofensor, ou seja, se o exercício do direito se deu dentro dos limites impostos pela própria lei e se não houve ofensa à dignidade da pessoa humana. Deverá pesar, também, como e onde a ofensa ocorreu, dimensionando os prejuízos materiais e morais atinentes ao caso concreto[42].

4.2 A responsabilidade objetiva, subjetiva e a aparente colisão entre legislações federais à luz do Tema 987

A discussão faz necessário ponderar a existência de três correntes de entendimento doutrinário que abordam o tema. A primeira entende pela isenção completa do provedor de aplicação, pois seria tão somente intermediário,

[41] KALLAJIAN, Manuela Cibim**. Privacidade, informação e liberdade de expressão**: conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 204.
[42] KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão**: conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019. p. 204-205.

defendendo-se a inexistência de nexo de causalidade entre o serviço e eventual dano suportado pela vítima.

Ocorre que o referido entendimento não se mostra mais uma possibilidade a ser adotada em território brasileiro, em razão de ter sido pacificada a conclusão de que todos os usuários da plataforma são classificados como consumidores. Isto porque, apesar das plataformas digitais não serem pagas, auferem significativo rendimento com o uso da plataforma.

A segunda corrente defende a responsabilização objetiva dos provedores, em consonância com o Código de Defesa do Consumidor, justamente pelos usuários serem classificados como consumidores. Esta é a tese utilizada pelo Tribunal Regional para concluir pela inconstitucionalidade do art. 19 do MCI e, portanto, pela responsabilização do Facebook Brasil no caso em comento.

De acordo com o acórdão do Tribunal Regional, condicionar a remoção à decisão judicial seria isentar por completo os provedores de aplicação de toda e qualquer indenização, de forma a inutilizar a medida protetiva garantida pelo Código de Defesa do Consumidor. Ademais, obrigaria o consumidor a ingressar em juízo para que o provedor adotasse providências que poderiam ser resolvidas extrajudicialmente, o que geraria um desequilíbrio no sopesamento entre a liberdade de expressão e o direito à intimidade, a vida privada, a honra e a imagem.

Ocorre que, como sabido, a responsabilidade objetiva deve ser considerada em caráter excepcional, em situações devidamente especificadas no ordenamento jurídico, de forma que admitir a responsabilidade objetiva dos provedores de aplicação em razão de ilícitos cometidos por terceiros, poderia implicar em uma nova modalidade de responsabilidade objetiva[43].

Antes mesmo do início de vigência do MCI, o STJ já havia proferido entendimento no sentido de ser inaplicável a responsabilidade objetiva a casos semelhantes, pois eventual dano moral decorrente de mensagens de conteúdo

[43] SILVEIRA, Sebastião Sérgio da; PERES, Edilon Volpi. Cidadania Digital: necessidade de ponderação entre os valores constitucionais relativos a proteção ao consumidor e aqueles contemplados na lei do marco civil da internet. **Revista da Faculdade de Direito da Ufg**, [S.L.], v. 43, p. 1-16, 21 abr. 2020. Universidade Federal de Goiás. http://dx.doi.org/10.5216/rfd.v43.57192. Disponível em: https://www.revistas.ufg.br/revfd/article/view/57192. Acesso em: 10 set. 2021.

ofensivo não constituiria risco inerente à atividade[44]. E, após a promulgação do MCI, o tema foi consolidado pela 4ª Turma do STJ, de forma a reconhecer a responsabilidade subjetiva dos provedores de internet em casos de veiculação por terceiros de conteúdo ilícito, pois também não teriam o dever de controle prévio dos conteúdos[45].

A terceira corrente doutrinária defende a responsabilidade subjetiva e possui duas ramificações: (i) a responsabilidade subjetiva dos provedores de aplicação da internet em razão da não adoção de providências ainda que após o envio de notificação extrajudicial e (ii) a responsabilidade subjetiva em razão do descumprimento de ordem judicial determinando a remoção do conteúdo considerado ilícito.

A responsabilidade em razão do não atendimento de notificação extrajudicial é a tese defendida pela parte autora no caso que originou o debate do Tema 987, aduziu que não era usuária da plataforma do Facebook e, mesmo ciente da existência do perfil falso mediante envio de notificação extrajudicial, não teria removido o perfil.

Ocorre que, caso esta tese prevalecesse, implicaria na concessão aos provedores de aplicação de internet do poder de analisar eventual ilicitude dos conteúdos, o que pela reserva de jurisdição seria autoridade tão somente do Poder Judiciário. Já a responsabilidade subjetiva em razão de descumprimento de ordem judicial de remoção é a aplicada atualmente com fulcro no ar. 19 do MCI.

O professor Marcelo Thompson[46] critica a aplicação da responsabilidade subjetiva nos termos do MCI, pois entende que há uma isenção de responsabilidade demasiada dos provedores de aplicação da internet, na medida em que não podem ser responsabilizados por conteúdos que violam direitos das pessoas, ainda que lucrem significativamente com as informações prestadas e estejam comprovadamente cientes da existência do ilícito.

---

[44] STJ**, REsp 1186616**, Rel. Min. Nancy Andrighi, J. em 23.08.2011, DJe. 31.08.2011

[45] STJ, 4ªT., **REsp 1.501.187/RJ,** Rel. Min. Marco Buzzi, J. em 16.12.2014, DJe 03.03.2015

[46] Thompson, Marcelo (2012). Marco civil ou demarcação de direitos? Democracia, razoabilidade e as fendas na internet do Brasil. **Revista De Direito Administrativo**, 261, 203–251. https://doi.org/10.12660/rda.v261.2012.8856.

Porém, neste ponto, destaca-se que o MCI não impede ou proíbe que os provedores de aplicação de Internet removam conteúdos, por iniciativa própria ou mediante notificação extrajudicial, desde que haja a verificação de violação aos termos de uso da plataforma, que nada mais é do que um contrato firmado entre as partes no ato do cadastro do usuário.

Inclusive, essencial a ressalva de que no caso de o provedor de aplicação de internet optar por remover conteúdos espontaneamente poderá, da mesma forma, ser responsabilizado por eventualmente violar o princípio da liberdade de expressão.

Nesse sentido, defende-se que o legislador teria optado conscientemente pela adoção de princípios norteadores capazes de garantir a vedação à censura e à liberdade de expressão e que eventual reconhecimento de inconstitucionalidade acarretaria na imposição a empresas privadas de controle, censura e restrição à comunicação, o que é constitucionalmente vedado.

O Ministro Ricardo Villas Bôas Cueva já manifestou entendimento no sentido de que não se poderia exigir dos provedores de aplicação a análise sobre se os conteúdos são ou não apropriados para divulgação pública, cabendo tão somente ao Judiciário, quando acionado, determinar se o conteúdo deve ser removido da rede mundial de computadores, bem como fixar eventual reparação civil em face do real responsável pelo ato ilícito.[47]

No que se refere ao possível conflito entre o Código de Defesa do Consumidor e o Marco Civil da Internet suscitado pelo Tribunal Regional, trata-se de uma antinomia aparente, a qual surge na medida em que há aparentes conflitos de normas quando da sua interpretação, o qual poderá, geralmente, ser solucionado pelos critérios hierárquico, da especialidade e cronológico.

Ambas as legislações possuem caráter federal, porém considerando o critério cronológico e da especialidade, haveria de prevalecer o artigo 19 do MCI, posto que mais recente e publicado especificamente para regular relações jurídicas no âmbito da internet.

[47] STJ, 3ª T**., REsp 1.568.935/RJ**, Rel. Min. Ricardo Villas Boas Cueva, j. 05.04.2016. DJe 13.04.2016

Nesse sentido, o Facebook, no bojo dos autos que tratam do Tema 987, defende que o Marco Civil da Internet não teria o condão de derrogar o Código de Defesa do Consumidor, mas de complementar no sentido de limitar a norma a casos de veiculação de conteúdos efetuado por terceiros por meio das plataformas, o que teria sido acolhido pelo Supremo Tribunal Federal ao, em outros casos, decidir pela prevalência do Marco Civil da Internet em detrimento do Código de Defesa do Consumidor, em casos de conflitos entra ambas as normas.

Assim, haveria um diálogo entre as normas, e não um conflito, pois o próprio Marco Civil da Internet tem como um de seus pilares a defesa do consumidor[48], bem como impõe a aplicação de normas de proteção e defesa do consumidor no âmbito das relações da internet.

O MCI dispõe sobre exceções à regra do artigo 19, quando prevê no artigo 21 que os provedores serão responsabilizados subsidiariamente

> pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Assim, questiona-se se não seria o caso de analisar a (in)constitucionalidade do referido dispositivo legal de forma mais restrita, isto é, apenas para os casos em que há alegação de perfil falso, como uma exceção a regra geral disposta pelo artigo 19, da mesma forma que há para os casos contendo cenas de nudez ou de atos sexuais.

Assim, de qualquer ângulo que se observe o debate, evidentemente acarreta a necessidade de sopesamento de princípios constitucionalmente protegidos de forma a contrapor a dignidade da pessoa humana e direitos de personalidade como a liberdade de expressão, a livre manifestação do pensamento, o livre acesso à informação e a reserva de jurisdição.

[48] BRASIL. **Lei n. 12.965**, de 23 de abril de 2014**, Art. 2º, V -** a livre iniciativa, a livre concorrência e a defesa do consumidor; Art. 7º, VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que

5 REFLEXÕES SOBRE A CONSTITUCIONALIDADE DO ARTIGO 19 DO MARCO CIVIL DA INTERNET

Nas situações narradas, verifica-se o que tem ocorrido regularmente no Brasil: a tutela posterior do Poder Judiciário – por provocação de entidades e pessoas de vários seguimentos – de direitos em demandas que implicam em ponderação sobre a liberdade de expressão, a remoção de conteúdo da internet ou, não sendo proposto ou aplicado esse mecanismo, o emprego de algum tipo de condenação negativa aos usuários de internet.

Em razão das evoluções da civilização da informação[49] – uso massivo das mídias sociais, direitos de liberdade de expressão e imprensa pela internet, trabalho remoto, exigência social de mais transparência pública, acesso e uso de dados pessoais, exigiu-se o debate e a construção de novas ferramentas para lidar com a dinâmica do exercício de direitos pelos cidadãos em meios virtuais, sempre projetando a plena participação social na construção do Estado Democrático de Direito.

Motivado por essas inovações, em 23 de abril de 2014, entrou em vigor o MCI. Tida como uma lei de vanguarda na proteção dos direitos e princípios fundamentais na internet, o Marco Civil inspirou outros países e inaugurou um modelo de regulamentação da rede inovador em conteúdo e forma[50].

No que diz respeito ao conteúdo, o Marco Civil estabeleceu princípios e direitos de usuários, apontando para uma espécie de "constituição da internet"[51]. Inclusive, há no Marco Civil um capítulo (Cap. IV) dedicado às diretrizes que devem pautar a atuação do Poder Público no desenvolvimento da internet, reforçando o uso de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática na rede por meio da coordenação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica atuando em sinergia. Como bem

[49] ZUBOFF, Soshana, 1951-. **A era do capitalismo de vigilância**: a luta por um futuro na nova fronteira de poder; tradução George Schlesinger. 1ª ed. – Rio de Janeiro: Intrínseca, 2020, p. 23.

[50] SOUZA, Carlos Affonso. LEMOS, Ronaldo. **Marco civil da internet**: construção e aplicação. Juiz de Fora: Editar Editora Associada Ltda, 2016.

[51] INTERNETLAB. **Especial Marco Civil 5 anos**: por que devemos celebrar. Disponível em: https://www.internetlab.org.br/pt/especial/especial-marco-civil-5-anos-por-que-devemos-celebrar/. Acesso em 10 de set. de 2021.

registrado na análise de Kimberly Anastácio[52], o MCI determinou a obrigatoriedade da adoção de uma cultura de participação social no processo de racionalização da gestão da rede. Isso afasta o controle indiscriminado da rede e a criminalização de comportamentos banais de usuários de internet.

No que tange à forma, a própria internet foi utilizada no processo de elaboração da Lei. O Marco Civil foi concebido a partir da abertura das bases do debate e mobilizou a sociedade à discussão, passando por uma fase de consulta pública na própria internet, por meio da qual cidadãos, ligados ou não a diversas organizações, apresentaram óticas distintas para o aperfeiçoamento do projeto.

Integrando-se ao plano mais geral de regulamentação das liberdades comunicativas, de pronto, em seu art. 2º, corroborado nos arts. 3º e 4º, o Marco Civil dispõe que "a disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão". No entanto, mais expressivo do que isso é a constatação de que a lei, com o nítido objetivo de "assegurar a liberdade de expressão e impedir a censura", estabeleceu um procedimento cauteloso para a remoção forçada de conteúdo, exigindo decisão judicial que especifique inequivocamente o material a ser removido, sob pena de nulidade. A intenção, portanto, foi assegurar o exame jurisdicional individualizado dos discursos que se pretende cercear – o que não guarda nexo com a lógica simplificadora de alterar o MCI via medida provisória, no supetão político.

Embora a aplicação da lei ainda seja bastante controversa, como no caso do bloqueio de aplicativos[53] ou das regras sobre a neutralidade de rede[54], ela tem se mostrado fundamental para a proteção e promoção da liberdade de expressão[55],

[52] ANASTÁCIO, Kimberly de Aguiar. Participação na governança da Internet: o multissetorialismo do Comitê Gestor da Internet no Brasil (CGI.br). **40º Encontro Anual da Anpocs.** Participação na governança da Internet: o multissetorialismo do Comitê Gestor da Internet no Brasil (CGI.br), 2016.

[53] BRASIL. STF, ADI 5527 e ADPF 403, relatadas pelos ministros Rosa Weber e Edson Fachin, respectivamente. "Segundo a Ministra Rosa Weber, Marco Civil da internet não permite que WhatsApp seja suspenso". Fonte: https://www.conjur.com.br/2020-mai-27/rosa-marco-civil-internet-nao-permite-whatsapp-seja-suspenso. Acesso em 11 de set. de 2021.

[54] "O principal objetivo do princípio da neutralidade da rede é preservar a arquitetura aberta da Internet". "A internet assemelha-se mais a uma praça do que um sistema de televisão". RAMOS, Pedro Henrique Soares. Arquitetura da Rede e Regulação: a Neutralidade da Rede no Brasil Fundação Getúlio Vargas, 2015.

[55] COSTA, Maria Cristina Castilho; BLANCO, Patricia. **Liberdade de expressão e seus limites**. [S.l: s.n.], 2015.

sendo um importante exemplo de norma progressista e positiva, inovadora em sua preocupação com a garantia dos direitos humanos *online*.

Antes da promulgação do MCI não existia jurisprudência uniforme sobre o tema; o entendimento dominante[56] era no sentido de reconhecer a responsabilidade do provedor de aplicação que deixava de adotar as providências para a remoção do conteúdo ilícito após o recebimento de notificação extrajudicial, não sendo necessária uma ordem judicial nesse sentido, ou seja, o sistema de notificação e retirada – "notice and takedown".

Entretanto, antes da aprovação MCI, ocorreram debates e até mesmo a realização de consultas públicas que, após inúmeras ponderações e sugestões, resultou na opção do legislador por privilegiar a liberdade de expressão e o repúdio à censura prévia, visando a liberdade de produção de conteúdo pelos usuários, sem a necessidade de aprovação prévia dos intermediários.

Dessa forma, considerando a importância da liberdade de expressão online e no intuito de evitar a censura e monitoramento de publicações, decidiu-se que a responsabilidade tem início quando do descumprimento do prazo determinado em ordem judicial específica, na forma como consta no artigo 19. E, do ponto de vista processual, para facilitar o acesso à Justiça, a lei assegura a possibilidade de o usuário ajuizar ação no Juizado Especial Cível (§ 3º do art.19) e de concessão de antecipação da tutela pelo juiz (§ 4º do art. 19).

Percebe-se, assim, que o que o MCI estabelece é que os provedores de aplicações serão responsabilizados apenas se não cumprirem ordem judicial para a retirada do material ofensivo. E isso não os impede de determinar requisitos para a remoção de conteúdo em seus termos de uso e considerem eventuais notificações enviadas pelas supostas vítimas de danos resultantes do conteúdo publicado.

Esse modelo, de propiciar a autorregulação dos provedores, visa combater a indústria das notificações para remoção de conteúdo em excesso, e privilegia a posição de defesa da liberdade de expressão, pois garante aos provedores a salvaguarda que amortece o temor que poderia existir no sentido de que a não

[56] BRASIL. STJ. **REsp nº 1186616/MG** (2010/0051226-3), Relatora Ministra Nancy Andrighi, 3ª Turma, DJe 31/8/2011.

remoção do conteúdo, depois da notificação, geraria automaticamente a sua responsabilização.

Ainda, a solução trazida pelo art. 19 não condiciona a parte interessada a necessariamente propor uma ação judicial para retirar o conteúdo, posto que isso dependerá de diversos fatores como o conteúdo divulgado, os termos de uso dos sites, o convencimento da notificação submetida pela parte, e direciona o equacionamento de uma eventual colisão, divergência entre vítima e provedor para o Judiciário. A norma reconhece que é justamente o Poder Judiciário a instância legítima para a resolução da questão, especialmente daquela mais complexa e de maior repercussão. Nessa direção, vale registrar a explicação de Renato Opice Blum, Paulo Sá Elias e Renato Leite Monteiro[57]:

> Importante destacar que apesar de em nenhum momento no projeto de lei se afirma que um conteúdo somente será retirado com ordem judicial, muitas vezes a interpretação dada a proposição acima é esta, de que será necessária uma ordem judicial para que o conteúdo seja removido. Não, o conteúdo poderá, também, ser retirado sem a prolação de ordem judicial, como nos casos em que este vai de encontro aos termos de uso de um serviço ou na existência de lei específica que regule a retirada de conteúdo determinado. Um serviço de aplicação tem a discricionariedade para escolher quais conteúdos aceitará em sua plataforma. E estas regras são aceitas pelos usuários ao iniciarem o uso dos serviços.

Percebe-se que o dispositivo do MCI cria um ambiente de interferência mínima em modelos de negócios dos provedores de aplicação de internet no Brasil ao determinar que a responsabilização civil somente poderá ocorrer após descumprimento de ordem judicial solicitando a remoção do conteúdo.

Ou seja, a ordem judicial leva à obrigatoriedade de exclusão, mas disso não se infere que somente com ordem judicial seria permitido excluir. Na explicação do professor Carlos Affonso Souza[58]:

---

[57] **Marco regulatório da internet brasileira**: "Marco Civil" disponível em https://www.migalhas.com.br/depeso/157848/marco-regulatorio-da-internet-brasileira---marco-civil. Acesso em 24 de set. de 2021.

[58] Souza, Carlos Affonso. De Teffé, Chiara Spadaccini. **Responsabilidade dos provedores por conteúdos de terceiros na Internet**. Consultor Jurídico. Disponível em: https://www.conjur.com.br/2017-jan-23/responsabilidade-provedor-conteudo-terceiro-Internet#sdfootnote-3sym. Acesso em 24 de set. de 2021.

> Já que não existe para os provedores de aplicações de internet o dever de monitoramento prévio, a notificação atua como um alerta para que os mesmos possam averiguar a procedência de um suposto dano e analisar a viabilidade da remoção do conteúdo questionado. Caso decidam remover o conteúdo por ser contrário aos termos de uso e demais políticas que regem o funcionamento da plataforma, os provedores não ofenderão o Marco Civil da Internet, visto que a lei não proíbe a exclusão de conteúdo nesses termos.
>
> Todavia, deve-se evitar que os provedores abusem de sua posição e filtrem ou realizem o bloqueio de conteúdos sem uma justificativa plausível, já que isso restringiria indevidamente a liberdade de expressão. Se isso ocorrer, ele poderá até mesmo ser responsabilizado diretamente por conduta própria. Como os provedores gozam de isenção de responsabilidade antes da ordem judicial, eles devem tomar o exercício da liberdade de expressão como vetor de suas atividades, sendo medidas de filtragem, bloqueios ou remoção uma solução excepcional.

O art. 19, da forma como foi posto, viabiliza soluções que albergam os interesses em jogo de modo a prestigiar a liberdade de expressão, direcionando o papel do provedor e assegurando-lhe uma função de destaque na prevenção e na eliminação de danos.

Nesse viés, o provedor de aplicações poderá recusar o pedido de remoção quando, por conta própria, entender que aquele conteúdo é protegido pela liberdade de expressão. O que complica é que, na ausência da garantia do art. 19, a mera possibilidade de vir a ser responsabilizado por não atender à demanda do usuário ofendido produzirá o que ficou conhecido como "efeito inibidor" (chilling effect)[59]. Isto é, os provedores são levados a remover o conteúdo que, a princípio, é lícito pelo receio de vir a ser responsabilizado futuramente pelo Judiciário.

O art. 19 não torna o ambiente virtual numa "terra sem lei", fazendo com que os usuários que praticam um ilícito não sofram consequências pelos seus atos. Pelo contrário, é pelo próprio MCI, em seu art. 15, que os provedores de redes sociais são obrigados a armazenar dados de seus usuários para, eventualmente, fornecê-los às autoridades policiais e/ou judiciárias a fim de que seja apurado qualquer ilícito.

[59] Kurtz, Lahis. Ameaças opacas à liberdade de expressão online: chilling effect e shadowban. Disponível em https://irisbh.com.br/ameacas-opacas-a-liberdade-de-expressao-online-chilling-effect-e-shadowban/. Acesso em 24 de set. de 2021.

O dispositivo também não abre espaço para discutir acerca da remoção daqueles casos em que a ilegalidade do conteúdo é evidente. Nas situações em que a ilicitude do conteúdo postado é inequívoca, o MCI determina que o provedor deve retirar esse conteúdo imediatamente, assim que tiver ciência da sua existência – art. 21. Por exemplo, se alguém publicar um vídeo contendo cenas de sexo não consentido Instagram, a vítima desse crime poderá, de forma direta, notificar a plataforma para a remoção do conteúdo.

Hoje, o ciberespaço ultrapassa a ideia de mero meio ou espaço de interação pública[60]; ele já é considerado um verdadeiro repositório de ideias e projetos que alimentam o debate público, como se percebeu na construção do MCI. Na concepção de Castells[61], as diversas formas de sociedade civil suscitam o debate público e desta forma podem ter influência sobre as decisões do Estado.

Os atuais conflitos acerca da regulação da moderação de conteúdo são comumente deflagrados em razão do grau de subjetividade dos conteúdos difundidos pelos usuários e da quantidade de informações suscetíveis de identificação pelos critérios que envolvem as tomadas de decisão da pretensa moderação[62].

As restrições empregadas por meio da moderação de conteúdo necessariamente perfazem algum tipo de processo cognitivo. A construção das bases de modulação de regras das comunidades do *facebook*, *twitter*, *youtube* e de outras mídias sociais são constantemente questionadas social[63] e judicialmente. Há uma movimentação social cada vez maior que requer das aplicações a formulação de regras claras na estruturação de mecanismos recursais, na apresentação de razões e justificativas para as decisões tomadas pelas empresas e, especialmente, na

[60] Solagna, F.; De Souza, R. H. V.; Leal, O. F. **Quando o ciberespaço faz as suas leis**: o processo do marco civil da internet no contexto de regulação e vigilância global. Vivência: Revista de Antropologia, v. 1, n. 45, 18 nov. 2015.

[61] CASTELLS, Manuel. The new public sphere: global civil society, communication networks, and global governance. **The ANNALS of the American Academy of Political and Social Science**, 2008, 616, p.78-93. Apud SOLAGNA, F.; DE SOUZA, R. H. V.; LEAL, O. F. Quando o ciberespaço faz as suas leis: o processo do marco civil da internet no contexto de regulação e vigilância global. Vivência: Revista de Antropologia, v. 1, n. 45, 18 nov. 2015.

[62] HARTMANN, Ivar A. DA SILVA, Lorena Abbas. Inteligência artificial e moderação de conteúdo: o sistema content id e a proteção dos direitos autorais na plataforma YouTube. **Ius Gentium**. Curitiba, vol. 10, n. 3, p. 145-165, set./dez. 2019.

[63] Políticas de comunidade do Facebook no Brasil têm trechos sem tradução para português – Estudo. Pesquisa do ITS identificou ao menos três trechos não traduzidos ou com traduções equivocadas. Disponível em https://nucleo.jor.br/curtas/2021-04-07-facebook-traducao-regras-comunidade. Acesso em 13 de set. de 2021.

transparência de dados e relatórios envolvendo o processo de moderação de conteúdo[64].

Um dos caminhos adotados pelo Facebook para diminuir os empasses sobre o tema e aumentar sua *accountability* foi a criação, em setembro de 2020, do Comitê de Surpevisão *Facebook Oversight Board*[65], um órgão independente da empresa com capacidade de promover mais previsibilidade e transparência quanto à moderação de conteúdo pela rede social. Houve até mesmo a concepção de um estatuto[66], um documento de base que rege o Comitê de Supervisão e descreve sua estrutura, define suas responsabilidades e seu propósito, e explica sua relação com o Facebook. Inclusive, há uma enorme expectativa quanto à decisão do *Oversight Board* sobre o pedido de revisão[67] do Facebook da decisão de suspender o ex-presidente dos Estados Unidos Donald Trump da plataforma em janeiro de 2021.

Percebe-se, portanto, que é necessário assegurar um ambiente favorável para a busca por soluções para o problema da moderação de conteúdo pelas plataformas que não selecionam previamente quem comunicará ou quais agendas serão divulgadas em suas páginas; e à autorregulação, tendo como motor a implementação de práticas de transparência, considerando que também é responsabilidade do setor público regular e impor obrigações nesse sentido.

---

[64] ESTARQUE, Marina. ARCHEGAS, João Victor. Redes Sociais e Moderação de Conteúdo: criando regras para o debate público a partir da esfera privada. Instituto de Tecnologia e Sociedade do Rio - ITS. Abril de 2021.

[65] "O objetivo do comitê é promover a liberdade de expressão por meio da tomada de decisões independentes e baseadas em princípios com relação ao conteúdo no Facebook e no Instagram e por meio da emissão de recomendações sobre a política de conteúdo relevante da empresa do Facebook. Quando estiver completo, o comitê será composto de aproximadamente 40 membros do mundo todo, que representarão um amplo conjunto de formações acadêmicas e origens. Esses membros poderão selecionar casos de conteúdo para análise e manter ou reverter as decisões do Facebook sobre conteúdo. O objetivo da criação do comitê não é ser uma simples extensão do processo de análise de conteúdo do Facebook que já existe. Em vez disso, ele analisará um número seleto de casos altamente emblemáticos e determinará se as decisões foram tomadas de acordo com as políticas e valores declarados pelo Facebook." Informação disponível na página inicial do https://oversightboard.com/. Acesso em 12 de set. de 2021.

[66] A íntegra do estatuto está disponível em https://oversightboard.com/governance/. Acesso em 12 de set. de 2021.

[67] Fonte: https://oversightboard.com/news/236821561313092-oversight-board-accepts-case-on-former-us-president-trump-s-indefinite-suspension-from-facebook-and-instagram/. Acesso em 12 de set. de 2021.

6 CONCLUSÃO

O presente trabalho teve como objetivo analisar a responsabilidade civil dos provedores de aplicação de internet por conteúdos ilícitos gerados por terceiros antes e após a vigência do Marco Civil da Internet, de maneira a trazer uma reflexão sobre os limites e condições da remoção de conteúdos ofensivos.

A internet é uma rede que impulsiona liberdades, sendo uma plataforma extraordinária para a liberdade de expressão, que pode, por este motivo, gerar danos em larga escala e de difícil contenção. Assim, este trabalho teve como problema de pesquisa responder os seguintes questionamentos: até que ponto determinadas manifestações estão resguardadas pela liberdade de expressão? Até que ponto exteriorizar certas convicções pode ser considerado ofensa à honra e à imagem? Se mostra constitucional o art. 19 do MCI e o modelo regulatório que condiciona a remoção de conteúdo à prévia ordem judicial?

A complexidade da temática repousa na proibição ou não dos conteúdos ofensivos à honra e à imagem frente a garantias do Estado Democrático de Direito de que a manifestação do pensamento é livre e deve ser protegida na mesma medida que outras garantias fundamentais. Além disso, muito se discute a respeito da constitucionalidade do art. 19 do MCI porque, dentre outras teses, a reparação da violação a direitos fundamentais estaria condicionada à propositura de ação judicial e à emissão de ordem judicial, o que seria contrário ao disposto no art. 5º, X e XXXV, da CF.

O debate a respeito do modelo de responsabilização civil dos provedores de aplicação de internet no Brasil deflagrou a interposição de vários recursos pelo País, dentre eles, destacam-se os RE nº 1.057.258/MG e RE nº 1.037.396/SP, reconhecidos pelo Supremo Tribunal Federal como Temas de Repercussão Geral.

Foi necessário primeiro compreender a importância da discussão dos Temas 533 e 987 sobre a remoção de conteúdos ilícitos gerados por terceiros por intermédio dos provedores de internet. Para isso, foi realizada uma breve análise dos andamentos processuais de ambos os recursos.

O Tema 533 versa sobre o dever de empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário, já o Tema 987 aborda a constitucionalidade do art. 19 da Lei nº 12.965/2014, que determina a necessidade de prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, websites e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros. Logo, o que difere os dois recursos é o fato do Tema 533 se referir à discussão da matéria antes da promulgação do Marco Civil da Internet, que, em decorrência disso, será julgado sob outro prisma.

Posteriormente, o objeto de estudo se deu acerca dos direitos constitucionais da personalidade e das liberdades constitucionais de informação e de expressão, seus conceitos, limites e importância para o Estado Democrático de Direito, bem como a colisão entre esses direitos fundamentais. Essa análise foi crucial para atingir o intuito do presente trabalho. Por meio desse estudo, foi possível observar que a colisão de princípios constitucionais ou de direitos fundamentais não se resolve mediante o emprego dos critérios tradicionais de solução de conflitos de normas.

Por fim, o presente trabalho se dedicou à análise da repercussão de cada Tema e as suas similitudes, verificando-se que o Tema 533 aborda a colisão entre direitos fundamentais, enquanto o Tema 987 trata da colisão entre legislações federais. Assim, a partir da análise dos Temas 533 e 987 de repercussão geral, este trabalho buscou solucionar o aparente conflito entre normas e direitos, chegando ao ponto principal do presente trabalho, abordando o método da ponderação, por meio do qual deve ser aplicado o princípio da proporcionalidade no caso concreto.

Os limites e condições sobre a remoção de conteúdos ofensivos encontram barreiras quanto à violação dos princípios constitucionais de liberdade expressão e de informação. No entanto, o ordenamento jurídico brasileiro não concede a essas garantias fundamentais um direito incontestável.

Verifica-se, portanto, o caráter não absoluto do direito fundamental à liberdade de expressão, apesar de sua grande importância para a manutenção da democracia, sendo necessária sua restrição quando o exercício desse direito extrapolar o direito do outro, muitas vezes ferindo sua honra, sua dignidade.

Dessa maneira, tendo em vista a eficiência do atual sistema de remoção de conteúdo, conclui-se que o Estado brasileiro, ao lidar com a regulação e condições para a retirada de conteúdos ilícitos e ofensivos na internet, deverá proporcionar aos provedores de aplicação de internet a análise dos casos concretos mais complexos a fim de observar se houve excesso no exercício do direito de expressar ou de informar que tenha violado algum direito.

REFERÊNCIAS

ASSEMBLEIA GERAL DA ONU. **Declaração Universal dos Direitos Humanos**. 217 A (III). Paris, 1948. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000139423.

BARROSO, Luís Roberto. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. **Revista de Direito Administrativo**, Rio de Janeiro, v. 235: 1-6, jan. 2004. p. 24. Disponível em: https://doi.org/10.12660/rda.v235.2004.45123.

BINICHESKI, Paulo Roberto. **Responsabilidade civil dos provedores de Internet**. Curitiba: Juruá, 2011.

BRANCO, Paulo Gustavo Gonet. Direitos Fundamentais em Espécie. In: MENDES, Gilmar Ferreira. **Curso de Direito Constitucional**. 9. ed. São Paulo: Saraiva, 2014.

BRASIL. Superior Tribunal de Justiça TJ, **Reclamação nº 5.498-PR**. Rel. Nancy Andrighi, j. 18.03.2011.

BRASIL. Superior Tribunal de Justiça, 3ª T., **Recurso Especial nº 1.568.935/RJ**, Rel. Min. Ricardo Villas Boas Cueva, j. 05.04.2016. DJe 13.04.2016.

_____. Superior Tribunal de Justiça, 4ªT., **Recurso Especial 1.501.187/RJ**, Rel. Min. Marco Buzzi, J. em 16.12.2014, DJe 03.03.2015.

_____. Superior Tribunal de Justiça, **Recurso Especial 1.186.616**, Rel. Min. Nancy Andrighi, J. em 23.08.2011, DJe. 31.08.2011.

_____. Supremo Tribunal Federal**. Resolução nº 663, de 12 de março de 2020.** Estabelece medidas temporárias de prevenção ao contágio pelo Novo Coronavírus (COVID19) considerando a classificação de pandemia pela Organização Mundial de Saúde (OMS).

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>

BRASIL. **Lei nº 12.965**. Marco Civil da Internet. Brasília, 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>

BRASIL. Lei nº 8.078. **Código de Defesa do Consumidor**. Brasília, 11 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário em relação ao Tema nº 987**, Relator Min. Dias Toffoli, Leading Case: RE 1037396.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário em relação ao Tema nº 533**, Relator Min. Luiz Fux, Leading Case: RE 1057258.

CANOTILHO, José Joaquim Gomes; MACHADO, Jónatas E. M.; JÚNIOR, Antônio Pereira Gaio. **Biografia não autorizada versus liberdade de expressão**. Curitiba: Juruá Editora, 2014.

CASTELLS, Manuel. The new public sphere: global civil society, communication networks, and global governance. The ANNALS of the American Academy of Political and Social Science, 2008, 616, p.78-93. *Apud* SOLAGNA, F.; DE SOUZA, R. H. V.; LEAL, O. F. Quando o ciberespaço faz as suas leis: o processo do marco civil da internet no contexto de regulação e vigilância global. Vivência: **Revista de Antropologia**, v. 1, n. 45, 18 nov. 2015.

CEROY, Frederico Meinberg. **Os conceitos de provedores no Marco Civil da Internet. 2014**. Disponível em: https://www.migalhas.com.br/depeso/211753/os-conceitos-de-provedores-no-marco-civil-da-internet.

COLAÇO, Hian Silva. **Responsabilidade civil dos provedores de Internet**: diálogo entre a jurisprudência e o marco civil da Internet. Revista dos Tribunais, Brasília, v. 957, julho de 2015. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.957.05.PDF.

COSTA, Maria Cristina Castilho; BLANCO, Patricia. Liberdade de expressão e seus limites. [S.l: s.n.], 2015.

DINIZ, Maria Helena. **Compêndio de introdução à ciência do direito**. 24. ed. São Paulo: Saraiva, 2013.

DINIZ, Maria Helena. Efetividade do direito a ser esquecido. **Revista Argumentum**, v. 18, n. 1, p.24, jan./abr. 2017. Disponível em: http://ojs.unimar.br/index.php/revistaargumentum/article/view/339.

FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. Direito & Internet III–Tomo II: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, p. 307-320, 2015.

GODOY, Cláudio Luiz Bueno de. **A liberdade de imprensa e os direitos da personalidade**. 2. ed. São Paulo: Atlas, 2008.

INTERNETLAB. **Especial Marco Civil 5 anos:** por que devemos celebrar. Disponível em: https://www.internetlab.org.br/pt/especial/especial-marco-civil-5-anos-por-que-devemos-celebrar/. Acesso em 10 de setembro de 2021.

KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão**: conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019

MEYER-PFLUG, Samantha Ribeiro**. Liberdade de Expressão e discurso do ódio**. São Paulo: Editora Revista dos Tribunais, 2009.

PADRÃO, Vinícius; SOUZA, Carlos Affonso. **Novos Contornos da Responsabilidade Civil dos Provedores de Aplicações de Internet por Conteúdo de Terceiros**. Direito do Consumidor: Novas Tendências e Perspectiva Comparada, Brasília: Editora Singular, 2019. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Direito_do_Consumidor%3Dnovas_tendencias.pdf#page=135.

PARENTONI, Leonardo Netto. Responsabilidade Civil dos Provedores de Serviços na Internet: Breves Notas. **Revista Magister de Direito Empresarial, Concorrencial e do Consumidor**. Porto Alegre: Magister, ano V, nº 25, p. 05-23, fev/mar. 2009. Disponível em: https://www.researchgate.net/profile/Leonardo_Parentoni2/publication/299801706_Responsabilidade_Civil_dos_Provedores_de_Servicos_na_Internet_Breves_Notas/links/5705610e08ae74a08e274a95/Responsabilidade-Civil-dos-Provedores-de-Servicos-na-Internet-Breves-Notas.pdf.

SILVEIRA, Sebastião Sérgio da; PERES, Edilon Volpi. Cidadania Digital: necessidade de ponderação entre os valores constitucionais relativos a proteção ao consumidor e aqueles contemplados na lei do marco civil da internet. **Revista da Faculdade de Direito da Ufg**, [S.L.], v. 43, p. 1-16, 21 abr. 2020. Universidade Federal de Goiás. http://dx.doi.org/10.5216/rfd.v43.57192. Disponível em: https://www.revistas.ufg.br/revfd/article/view/57192. Acesso em: 10 set. 2021.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 92.

SCHREIBER, Anderson. **Marco Civil da Internet**: avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. LUCCA,

Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira. Direito e Internet III: Marco Civil da Internet, Lei, n. 12.965, p. 277-305, 2014.

THOMPSON, Marcelo (2012). Marco civil ou demarcação de direitos? Democracia, razoabilidade e as fendas na internet do Brasil. **Revista De Direito Administrativo**, 261, 203–251. https://doi.org/10.12660/rda.v261.2012.8856.

ZUBOFF, Soshana, 1951. **A era do capitalismo de vigilância**: a luta por um futuro na nova fronteira de poder; tradução George Schlesinger. 1ª ed. Rio de Janeiro: Intrínseca, 2020.

A REQUISIÇÃO DE "DADOS CADASTRAIS DE IP" EM INQUÉRITOS CRIMINAIS SEM ORDEM JUDICIAL: UMA ANÁLISE CRÍTICA À LUZ DO MARCO CIVIL DA INTERNET

Édio Henrique de Almeida José e Azevedo[1]

RESUMO

Com frequência, provedores de acesso à internet são instados por autoridades policiais e do Ministério Público a informarem os "dados cadastrais de IP" de seus usuários, a despeito de ordem judicial para tanto. Tais requisições objetivam que o prestador indique os dados pessoais de usuário que navegava a partir de certo endereço IP, em determinado dia e horário. A partir da diferenciação entre os conceitos de "dados cadastrais" de "registros de acesso", a proposta deste trabalho é analisar a legalidade de tal expediente investigatório à luz do Marco Civil da Internet e da recém-promulgada Lei Geral de Proteção de Dados.

Palavras-chave: Privacidade dos Usuários de Internet. Quebra de Sigilo de dados telemáticos. Inquérito Penal. Marco Civil da Internet. Lei Geral de Proteção de Dados.

ABSTRACT

Internet access providers are frequently urged by law enforcement authorities to inform the "IP registration data" of their users, despite a court order to do so. Such requests aim for the provider to indicate the personal data of a user who was browsing from a certain IP address, on a certain day and time. From the differentiation between the concepts of "registry data" and "access records", the purpose of this paper is to analyze the legality of such investigative expedient considering the Brazilian Internet Civil Rights Act (Law nº 12.965, 2014) and the recently enacted Brazilian General Data Protection Act (Law nº.13.709, 2018).

Keywords: Internet user privacy. Disclosure of Internet Protocols (IP) records to police authorities - Internet Service Providers (ISPs). Criminal Procedure. Brazilian

[1] Advogado. Bacharel em Direito pela Universidade Federal de Minas Gerais. MBA em Direito da Economia e da Empresa pela Fundação Getúlio Vargas. Pós-graduando em Direito Digital: Inovação e Tecnologia, pelo UNICEUB. SHIS, QI 09, Conj. 17, Casa 14, Brasília – DF. edio@ea.adv.br

Internet Civil Rights Act (Law nº. 12.965, 2014). Brazilian General Data Protection Act (Law nº. 13.709, 2018)

1 INTRODUÇÃO

Nos últimos anos**,** o uso da internet vem assumindo um papel cada vez mais preponderante cotidiano dos brasileiros. Conforme relatório da Agência Nacional de Telecomunicações - ANATEL[2], entre os anos de 2017 e 2019, o número de usuários de internet banda larga fixa saltou de 8,26 milhões para 32,68 milhões de brasileiros. Um crescimento de 296%.

A tal fenômeno atribui-se a confluência de fatores diversos: no plano interno, assistiu-se à capilarização da oferta dos serviços de internet banda larga fixa, capitaneada, sobretudo, pela emergência de ISP[3]s de atuação regional - os chamados *Provedores de Pequeno Porte*[4], ou, *PPPs*[5], responsáveis por levar o serviço de internet de banda larga a muitos dos municípios do interior do País.

Há de se destacar nesse período a atuação governamental, em especial do Poder Executivo Federal, com a profusão de iniciativas voltadas à expansão da infraestrutura e à universalização do acesso à *internet* banda larga no país, temáticas estas que também passaram à pauta da ANATEL, atraída pela *"força gravitacional da banda larga*"[6]. No campo legislativo, destaca-se a promulgação do Marco Civil da Internet, em 2014. Em âmbito global, viu-se o desenvolvimento dos meios tecnológicos de transmissão – em especial da fibra óptica - e a rápida integração entre os serviços de internet à telefonia móvel, inclusive no Brasil, com a promoção

[2] *Relatório de acompanhamento do setor de telecomunicações*. Agência Nacional de Telecomunicações. Brasília, 2019. Acessado em https://www.telesintese.com.br/wp-content/uploads/2016/08/Relatorio-de-acompanhamento-da-Banda-Larga-1T16.pdf em 28/09/2021.

[3] Acrônimo para *Internet Service Provider.*

[4] *Art. 4º [...] XV - Prestadora de Pequeno Porte: Grupo detentor de participação de mercado nacional inferior a 5% (cinco por cento) em cada mercado de varejo em que atua*. (Res. Anatel nº 600/2012 – Plano Geral de Metas de Conexão).

[5] *"Estima-se que os ISPs regionais foram responsáveis pela maior parte do aumento das assinaturas de fibra óptica até a casa do cliente (fibre-to-the-home - FTTH) nos últimos anos." (*OCDE, **Avaliação da OCDE sobre Telecomunicações e Radiodifusão no Brasil 2020**, OECD Publishing, Paris, 2020 https://doi.org/10.1787/0a4936dd-pt.)

[6] "Enquanto o segundo e terceiro quinquênio de existência da ANATEL foram carregados de medidas de gestão de espectro, de políticas de expansão da infraestrutura de suporte à banda larga [...]" (ARANHA, Mário Iório, *A força gravitacional da banda larga*. In **Revista de Direito Estado e Telecomunicações** 3 (1): 1-42, 2011.)

do SMP de quarta geração (4G) a partir de 2014 e, mais recentemente, a chegada do SMP de quinta geração (5G).

A conjunção destes e outros fatores possibilitou a oferta de internet banda larga de alta qualidade a preços competitivos, resultando na inserção de milhões de brasileiros, de todas as classes sociais, na Era Digital.

A partir da difusão das redes *wireless* e da popularização do 4G, é possível afirmar que estar conectado à internet tornou-se uma constante no dia a dia de quase todos os brasileiros, conforme apontado na Pesquisa Nacional por Amostra de Domicílios Contínua - PNAD Contínua, divulgada pelo IBGE em 2018, onde se observou que no período compreendido entre 2016 a 2018, cresceu a ponto de atingir 99,2% dos domicílios em que havia telefone móvel celular.[7]

Para além do *acesso*, o constante desenvolvimento e adesão às aplicações baseadas na internet permitiram que a rede ultrapassasse a funcionalidade de meio de comunicação, tornando-se central e indispensável em diversas novas esferas da vida cotidiana, ressignificando e até substituindo completamente serviços tradicionais, como *bancos, educação e transporte de passageiros*. A partir das novas funcionalidades virtuais, emergem novos hábitos, hobbies e carreiras profissionais que formam a chamada "Sociedade em Rede", assim descrita por MANUEL CASSELS, em seu clássico *O Poder da Comunicação*:

> "Com mais de 2,8 bilhões de usuários de dispositivo de comunicação sem fio, redes horizontais de comunicação digital se tornaram a espinha dorsal de nossas vidas, materializando uma nova estrutura social que identifiquei anos atrás como sendo a sociedade em rede"[8]

Na mesma medida em que a internet passa a concentrar grande parte do fluxo de dados e documentos, é natural e previsível que emerjam igualmente também novas práticas reprováveis, que, valendo-se desses meios, lesam ou colocam em risco os bens jurídicos tutelados em nosso ordenamento.

---

[7] BRASIL. Instituto Brasileiro de Geografia e Estatística. **Relatório Tecnologia da Informação e *Comunicação -TIC*** *Pesquisa* Nacional por Amostra de Domicílios Contínua - PNAD Contínua, 2018. Disponível em: <https://www.ibge.gov.br/estatisticas/sociais/habitacao/17270-pnad-continua.html?=&t=downloads>. Acesso em 28 set. 2021.

[8] CASTELLS, Manuel. O Poder da Comunicação. – 3ª ed. São Paulo/Rio de Janeiro: Paz e Terra, 2019.

É neste novo campo de batalha que se coloca um desafio hercúleo: combater e práticas lesivas perpetradas pelos meios virtuais – seja pela constante criação e adaptação da legislação penal, seja aparelhando o aparato policial e investigatório para atuarem nesta nova realidade.

A prática descrita a seguir – cujo exame de sua legalidade é o tema central dentre trabalho – exemplifica tal desafio: a fim de conhecem a identidade de determinado usuário de internet o qual é suspeito de prática delituosa, autoridades policiais, requisitam os provedores de internet a fornecerem os "*dados de cadastrais de IP"* referentes ao usuário que estava conectado a partir de endereço IP em tais datas e horas, sendo tais requisições feitas diretamente às empresas provedoras, sem ordem judicial prévia.

2 A REQUISIÇÃO DE 'DADOS CADASTRAIS DE IP" EM INQUÉRITOS CRIMINAIS SEM ORDEM JUDICIAL. A SISTEMÁTICA DE REQUISIÇÃO DE DADOS PREVISTA NO MARCO CIVIL DA INTERNET (LEI Nº 12.965/2014) À LUZ DO PRINCÍPIO DA RESERVA DE JURISDIÇÃO

O artigo 5º, XII, da Constituição de 1988, garante o sigilo das correspondências, comunicações telegráficas, dados e comunicações telefônicas, inviolabilidade esta que somente por ser excepcionada, em último caso, em face de ordem judicial. Esta garantia constitui um dos pilares que sustentam a própria liberdade de pensamento e de expressão – isto é, o direito a externalizar uma opinião a quem quiser e pelo meio que quiser, tornando-a pública somente se assim desejar. Caso não houvesse tal garantia, os cidadãos não teriam liberdade de se manifestarem, sob medo de constante vigilância externa ou de represálias em decorrência de sua permissão, na lição de José Afonso da Silva[9].

É reconhecidamente árdua a tarefa das autoridades policiais: a cada novo dia, novas técnicas de informática são engendradas com fins não apenas na consecução da prática criminosa, mas sobretudo da preservação da anonimidade dos criminosos,

[9] "A liberdade de comunicação consiste num conjunto de direitos, formas, processos e veículos, que possibilitam a coordenação desembaraçada da criação, expressão e difusão do pensamento e da informação. É o que se extrai dos incisos IV, V, IX, XII e XIV do art. 5º" (SILVA, José Afonso da Silva. **Curso de Direito Constitucional Positivo.** – 20ª ed. rev. atual. Malheiros, São Paulo, 2001)

de modo a obstaculizar que as autoridades possam levá-los ao banco dos réus. É exatamente a busca por anonimidade tornam atrativo, por exemplo, o uso das criptomoedas para fins de lavagem de dinheiro, ocultação de bens e evasão de divisas, por exemplo. Afinal, como identificar quem está por trás da tela? Um caminho de investigação promissor é, de fato, a partir do endereço IP (*internet protocol*).

Conforme conceitua o art. 3º, III, do Marco Civil da Internet, o Endereço IP é o "*código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais".* Isto é, todo terminal conectado à internet ou a uma rede privada, é identificável a partir deste código numérico, chamado de IP. Porém, apesar de ser possível afirmar que cada terminal se conecta à rede a partir de um Endereço IP, a recíproca não é verdadeira, sendo comum a utilização de tecnologias, tal com o NAT/CGNAT que permitem que centenas de usuários estejam simultaneamente conectados a partir de um mesmo Endereço IP.

Atento ao comando constitucional, o Marco Civil da Internet garante sigilo aos usuários, bem como a inviolabilidade de suas comunicações, salvo, claro, por ordem judicial. Estas garantias estão elencadas ao art. 7º do diploma:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, **salvo por ordem judicial**, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, **salvo por ordem judicial**; (grifamos)

E caso ainda reste alguma dúvida da consonância entre a lei e a Carta Magna, basta volvermos ao artigo 10 daquela Lei:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput,

> de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

Vale aclarar que, em seu art. 3º, VI, o Marco Civil da Internet conceitua "registros de conexão", como "o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados", de modo a limar quaisquer dúvidas quanto aos dados albergados pelo direito ao sigilo.

Diante do exposto até aqui, é enganosa, a nosso ver, a percepção de que o Marco Civil da Internet, acaba por obstaculizar o combate aos crimes virtuais e a identificação de delinquentes ao garantir o direito à privacidade dos usuários. Uma análise apurada da norma nos leva a concluir em sentido contrário. É o que se vê do seu art. 13:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
>
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
>
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
>
> § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.
>
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º , que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º .

O Marco Civil da Internet não obstaculiza o desenvolvimento do combate aos crimes virtuais, pelo contrário, ele potencializa as chances de que as autoridades encontrem provas e identifiquem os infratores. Prova disso é o comando do § 2º, o qual dá prerrogativa à autoridade que diretamente exija do provedor que faça a guarda dos dados de registro em segurança por até 60 (sessenta dias), prazo razoável

para o ingresso e a apreciação de um pedido de quebra de sigilo. Logo, em verdade, tal dispositivo permite que o delegado/promotor desenvolva seu inquérito ciente de que, caso seja necessário requerer a quebra de sigilo, tais dados estão seguros, em ambiente controlado, que e poderão ser aproveitados oportunidade na apuração dos delitos.

E, embora o artigo 5º, XII, da CF/1988 seja taxativo quanto à ordem judicial como única hipótese excepcional à inviolabilidade, não faltam diplomas normativos a desafiar tal comando constitucional, seja para gerar novas exceções ou para relativizar a exigência de ordem judicial prévia, valendo-se de recursos hermenêuticos ou, sob a justificativa de dar celeridade e efetividade ao combate à criminalidade, buscam contemporizar a imprescindibilidade da reserva jurisdicional. Como bem destaca JACQUELINE DE SOUZA ABREU:

> Para além dessa hipótese interpretativa, e ao mesmo tempo que historicamente se resguardou a proteção do sigilo a esses tipos de dados, sempre houve também no direito brasileiro certa tentativa de delimitação jurídica de situações que não se configurariam 'quebra de sigilo' e de hipóteses excepcionais em que a 'quebra de sigilo" desses dados pessoais seria justificada, notadamente no que diz respeito ao franqueamento de acesso a esses dados para autoridades estatais, inclusive policiais.[10]

É nesse exato sentido a determinação constante da Lei nº 13.344, de 2016, que promoveu alteração no Código de Processo Penal para criar uma hipótese autorizativa tácita de quebra de sigilo telemático caso o Juiz não apreciasse o pedido em até 12 horas:

> Art. 13-B. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso. [...]
>
> (...)
>
> § 4º Não havendo manifestação judicial no prazo de 12 (doze) horas, a autoridade competente requisitará às empresas

[10] ABREU, JACQUELINE DE SOUZA. *Tratamento de Dados Pessoais para Segurança Pública: Contornos do Regime Jurídico Pós-LGPD.* In **Tratamento de proteção de dados pessoais.** Doneda, Danilo [et al] – Rio de Janeiro: Forense, 2021.

> prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, com imediata comunicação ao juiz.[11]

Ainda mais cristalino é o comando prescrito ao artigo 10, §1º do referido diploma:

> Art. 10. A guarda e a disponibilização dos **registros de conexão** e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º

Desse modo, vê-se que a imprescindibilidade da reserva judicial não é excesso de cautela do legislador constituinte ou desconsideração com a necessidade de pronta intervenção no combate ao crime, decorre da própria sistemática jurídica brasileira. Ao contrário. Quando uma autoridade policial requer uma diligência que implique na quebra de sigilo, estão em conflitos dos princípios igualmente positivados e juridicamente eficazes, de um lado, a garantia constitucional ao sigilo e, de outro, o dever do Estado de promover o direito à segurança pública.

Portanto, toda quebra de sigilo implica no afastamento – ainda que casuístico e pontual – da garantia constitucional, por isso, somente é tolerável "*em último caso*", cabendo ao magistrado o dever de, ao deferir a quebra, afastar a garantia constitucional do sigilo tão somente na medida necessária à consecução da finalidade da medida, devendo ser rechaçadas a total devassa da vida privada dos atingidos. Este sopesamento de princípios, à luz das lições de Alexy, vem sendo exercido pelo E. STF ao apreciar as muitas requisições medidas de quebra de sigilo de dados requeridas oriundas da CPI da Pandemia, cabendo aos ministros e ministras

[11] A constitucionalidade deste dispositivo está sendo questionada por meio da ADI 5.642, ajuizada pela Associação Nacional das Operadoras Celulares (ACEL).

negá-las quando excessivamente amplas ou desconexas dos fatos investigados[12]. No sistema penal brasileiro, este papel ao juiz de garantias, que possui o necessário distanciamentos do fato e das partes apreciar se a quebra requisitada se mostra necessária e, em caso positivo, em quais medida deverá ser executada. É a ordem prevista no Código de Processo Penal:

> Art. 3º-B. O juiz das garantias é responsável pelo controle da legalidade da investigação criminal e pela salvaguarda dos direitos individuais cuja franquia tenha sido reservada à autorização prévia do Poder Judiciário, competindo-lhe especialmente: [...] XI - decidir sobre os requerimentos de [...] b) afastamento dos sigilos fiscal, bancário, de dados e telefônico;

É interesse anotar, em conclusão ao item, que o próprio *parquet* federal vem mostrando preocupação com a constitucionalidade de práticas investigativas que, como no caso aqui analisado, são conduzidas sem a oitiva prévia do órgão, a quem cabe, no mais das vezes, a propositura de ação penal. O tema é tratado na ADPF 847/ DF, ajuizada pelo Procurador Geral da República em 24/05/2021, a ser julgada pelo STF. Para melhor contextualização, citamos excerto da peça inicial:

> "Demonstrar-se-á que os dispositivos impugnados, na medida em que possibilitam interpretação que permita a determinação de diligências policiais constritivas de direitos na fase investigativa, de ofício ou mediante representação da autoridade policial, sem o requerimento ou a manifestação prévia do Ministério Público, violam o sistema penal acusatório e os arts. 5º, LIV (deveres de inércia e de imparcialidade do magistrado que derivam do princípio do devido processo legal substantivo), 103, § 1º (oitiva prévia do Procurador-Geral da República em todos os processos de competência do STF), e 129, I, VII e VIII (funções institucionais do Ministério Público de promover privativamente a ação penal pública, exercer o controle externo da atividade"[13]

Diferente é o tratamento legal referente aos *dados cadastrais* dos usuários de internet. Estes sim - ao contrário do que ocorre com os dados de registro de conexão - podem ser requisitados aos provedores de acesso à internet, diretamente pelas autoridades investigatórias, sem necessidade de ordem judicial prévia, na forma da sistemática descrita no Decreto 8.771, de 2016:

[12] MS: 37972 DF; MS: 37972 DF, MS: 37962 DF, MS: 37971 DF.
[13] Petição Inicial, ADPF 847/DF.

> Da requisição de dados cadastrais
>
> Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014 , indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.
>
> § 1º O provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados.
>
> § 2º São considerados dados cadastrais:
>
> I - a filiação;
>
> II - o endereço; e
>
> III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.
>
> § 3º Os pedidos de que trata o caput devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.

Assim, o requerimento dados cadastrais referente ao fornecimento de dados de usuários específicos, logo, já identificados – como resta nítido no § 3º supracitado, não implica em quebra de sigilo e, portanto, dispensa a ordem judicial prévia, devendo tal requisição ser atendida pelo prestador de acesso à internet.

Logo, vê-se a relevância do tema aqui trazido, sendo patente a necessidade de aprofundamento da análise da legalidade de tal expediente investigatório, utilizado frequentemente pelas autoridades policiais.

A nosso ver, carece de embasamento legal a requisição de *"dados cadastrais de IP"*, uma vez que, como demonstrado, IP é um código numérico, e não um *"indivíduo"* (art. 11, § 3º, do Decreto 8.771, de 2016) muito menos um "usuário". Sendo assim, não parece adequada a solicitação de "dados cadastrais de IP". Afinal, o IP não tem pai nem mãe, qualificação ou profissão. Dados cadastrais se referem a dados pessoais, conceituados na forma do art. 5º, I, da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 2018:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

De tal modo, é forçoso concluir que a requisição de "dados cadastrais de IP", em verdade, se utiliza de uma construção textual para, de fato, ultrapassar a reserva

jurisdicional estabelecida pelo legislador constituinte, a fim de identificar os suspeitos de delitos virtuais sem precisar de aval judicial prévio.

Impõe destacar que parte da doutrina discorda do comando legal, sem, no entanto, deixar de reconhecer sua imperatividade. A crítica principal à indispensabilidade de ordem judicial é a alegação de que a exigência de autorização judicial prévia, muitas vezes é morosa ao ponto de colocar em risco a própria a eficiência perquisição penal. Nesse sentido, Patrícia Peck:

> A lógica trazida por este marco legal impôs um grande custo à sociedade, visto que também na investigação da autoria há necessidade de se socorrer do Judiciário, pois toda e qualquer informação relacionada aos logs de conexão e aos logs de navegação só pode ser apresentada mediante ordem judicial. A redação da lei acabou por cercear a atuação da própria autoridade policial e do Ministério Público, sujeitos a apenas poderem solicitar a preservação da prova digital mas sem autonomia para requisitar a sua apresentação.[14]

Assim é que nos parece inapropriado a autoridade responsável pela investigação valer-se de uma redação confusa, com entroncamento de conceitos bem definidos em lei com fim de driblar o comando positivado, exigindo diretamente de particular que faça algo que a lei não o obriga a fazer. E, pior, potencialmente expondo a identidade de centenas de usuários sem qualquer indício que os atrele aos fatos investigados.

3 CONCLUSÃO

Como restou demonstrado, a prática de requisições de "dados cadastrais de IP" dirigidas a provedores de acesso a internet sem ordem judicial não se amolda à ordem constitucional e à sistemática específica erigida pelo Marco Civil da Internet.

Além da ilegalidade em si, que já justificaria a cessação de tal prática, conclui-se que ela tampouco está alinhada com diversos outros institutos basilares da ordem constitucional, tal como o foro por prerrogativa de função. Não bastasse, em razão do difundido uso de CGNAT/NAT, e outras tecnologias que permitem o compartilhamento de endereços IP, tais diligências pode levar ao indevido indiciamento de grande número de usuários sem qualquer relação com os fatos

[14] PINHEIRO, Patrícia Peck. **Direito digital**. 5ª ed. São Paulo: Saraiva, 2013.

investigados no inquérito. Ademais, a quebra de sigilo desamparada de ordem judicial pode levar à inutilização de todo o inquérito, tornando inócuo o esforço empregado da persecução criminal.

REFERÊNCIAS

ABREU, JACQUELINE DE SOUZA. Tratamento de Dados Pessoais para Segurança Pública: Contornos do Regime Jurídico Pós-LGPD. In **Tratamento de proteção de dados pessoais**. Doneda, Danilo [et al] – Rio de Janeiro: Forense, 2021.

ANATE*L*. **Relatório de acompanhamento do setor de telecomunicações**. Brasília, 2019. Acesso em Disponível em: <https://www.telesintese.com.br/wp-content/uploads/2016/08/Relatorio-de-acompanhamento-da-Banda-Larga-1T16.pdf> Acesso em: 28 set. 2021.

ARANHA, Mário Iório, A força gravitacional da banda larga. In **Revista de Direito Estado e Telecomunicações** 3 (1): 1-42, 2011

BRASIL. Instituto Brasileiro de Geografia e Estatística. **Relatório Tecnologia da Informação e *Comunicação-TIC*** Pesquisa Nacional por Amostra de Domicílios Contínua -PNAD Contínua, 2018. Disponível em: <https://www.ibge.gov.br/estatisticas/sociais/habitacao/17270-pnad-continua.html?=&t=downloads> Acesso em 28 set. 2021.

CASTELLS, Manuel. O Poder da Comunicação. – 3ª ed. São Paulo/Rio de Janeiro: Paz e Terra, 2019.

OCDE, **Avaliação da OCDE sobre Telecomunicações e Radiodifusão no Brasil 2020**, OECD Publishing, Paris, 2020 https://doi.org/10.1787/0a4936dd-pt.)

OLIVEIRA, Eugênio Pacelli. Curso de processo penal. -18ª ed. rev. e ampl – São Paulo, Atlas, 2014

PINHEIRO, Patrícia Peck. **Direito Digital**. 5ª ed. São Paulo: Saraiva, 2013.

SILVA, José Afonso da Silva. **Curso de Direito Constitucional Positivo.** – 20ª ed. rev. atual. Malheiros, São Paulo, 2001

ANÁLISE ESTATÍSTICA DAS NOTÍCIAS FALSAS (FAKE NEWS) E DA RESPONSABILIDADE DE SEUS CRIADORES E COMPARTILHADORES

Eduardo Oesterreich da Rosa[1]

RESUMO

Passado a era industrial, surge, então, a era da informação ou, como mais conhecida, era digital. A informação que antes demorava para chegar, hoje transformou-se em questão de milésimos de segundos, dependendo de sua internet. As fontes foram cada vez mais ampliadas, o que antes eram apenas jornais, revistas, televisão e rádio, passou a não ser só elas, mas, também, a internet e seus recursos de informação e serviços. A grande vantagem dessa diversidade de fontes é a variedade de como o assunto pode ser abordado, seja ela de maneira mais formal, informal, com imparcialidade, sem imparcialidade e muitos outros. Dessa forma, a notícia deixa de ser apenas aquilo que as antigas mídias queriam que seus espectadores vissem, para ser algo mais perto da realidade. Entretanto, uma evolução na comunicação trouxe consigo também o outro lado da verdade, as chamadas Fake News ou notícias falsas. O presente artigo visa analisar qual seria a responsabilidade de quem cria e compartilha uma notícia falsa e a análise das estatísticas das notícias falsas. Para isso, o método utilizado foi o indutivo, pela realização de enquete para ter um conhecimento da visão das pessoas sobre a reponsabilidade de quem cria e quem compartilha uma notícia falsa e a análise de dados, e o método comparativo, analisando o posicionamento das normas e da jurisprudência. Conclui-se, ao final, que embora trata-se de uma coisa que acontece diariamente na vida das pessoas, a regulamentação ainda não conseguiu acompanhar de forma completa as faces da nova era da informação.

Palavra-chave: Notícias falsas. Criação e compartilhamento. Responsabilidade.

ABSTRACT

After the industrial age, then, the information age or, as it is better known, the digital age. The information that used to take time to arrive is now transformed in a matter of milliseconds, depending on your internet. The sources were increasingly

[1] Graduado em Direito. Aluno do curso pós-graduação lato sensu do Centro Universitário de Brasília-UniCEUB/ICPD

expanded, which before were just newspapers, magazines, television and radio, became not only them, but also the internet and its information resources and services. The great advantage of this diversity of sources is the variety of how the subject can be approached, be it in a more formal, informal way, with impartiality, without impartiality and many others. In this way, the news is no longer just what the old media wanted their viewers to see, to be something closer to reality. However, an evolution in communication also brought with it the other side of the truth, the so-called Fake News or false news. This article aims to analyze the responsibility of those who create and share a false news and the analysis of false news statistics. For this, the method used was the inductive one, by conducting a survey to gain knowledge of people's views on the responsibility of those who create and share false news and data analysis, and the comparative method, analyzing the positioning of norms and jurisprudence. It is concluded, in the end, that although this is something that happens daily in people's lives, the regulation has not been able to completely follow the faces of the new information age.

Keyword: False news. Creation and sharing. Responsibility.

1 INTRODUÇÃO

Antigamente não existia a quantidade de informações disponíveis que existem hoje. A era digital trouxe consigo uma maior proximidade das notícias, sendo abordada de diferentes formas e extremamente acessível. O que antes era necessários esperar para ver no noticiário da televisão ou no jornal do dia seguinte, hoje basta acessar os meios digitais que já encontra de forma atualizada a informação.

A notícia começou a ser espalhada da forma tão rápida que em questão de segundos a população toda já está sabendo do que aconteceu. Infelizmente, assim como acontecia desde o início das sociedades, as notícias falsas também são encontradas até hoje. Pessoas que inventam e que compartilham alegações desprovidas de veracidade e que acabam sendo consideradas como se verdade fosse.

O presente artigo visa analisar qual seria a responsabilidade desses criadores e compartilhadores de notícias falsas. Para isso, os objetivos específicos são: entender o conceito e a motivação das notícias falsas; analisar as estatísticas e as consequências de uma notícia falsa; a opinião pública sobre a responsabilidade do uso de notícias falsas e os obstáculos encontrados; e qual seria o posicionamento do ordenamento jurídico.

Parte-se da hipótese de que o ordenamento jurídico brasileiro ainda não estabeleceu de completa qual seria a responsabilidade de quem cria uma notícia falsa e quem a compartilha.

O método utilizado foi o indutivo, pela realização de enquete para ter um conhecimento da visão das pessoas sobre a reponsabilidade de quem cria e quem compartilha uma notícia falsa e a análise de dados, e o método comparativo, analisando o posicionamento das normas e da jurisprudência.

Ao final, apresenta-se os resultados e as conclusões dos objetivos e da hipótese proposta nesse artigo.

2 FAKE NEWS

2.1 Conceito e motivação

Buscar uma data para o surgimento das notícias falsas é extremamente difícil, tem quem acredita que começou juntamente com o surgimento da própria sociedade. Entretanto, seu conceito é de fácil compreensão, trata-se de uma informação que não representa a realidade[2].

Advento das redes sociais, as falsas informações, mais conhecido pela expressão Fake News, tornaram-se cada vez mais presente na era da informação. Os motivos que levam a criação dessas noticiam falsas são diversos. O mais comum é para manipular, mais negativamente do que positivamente, a opinião do público sobre alguma celebridade, políticos, e até mesmo pessoas comuns.

> O que instiga a prática são basicamente motivos torpes, tais como: a intenção de manchar a imagem de pessoas, tanto as físicas quanto as jurídicas, interesses econômicos, políticos, ou simplesmente pelo prazer de disseminar boatos ou notícias que causem alvoroço[3].

[2] Significados. **Fake News**. Disponível em: < https://www.significados.com.br/fake-news/> Acesso em 17 de set. 2021

[3] CASTRO, Paulo Tiago de. **Fake News, o Direito e as Providências**. Jusbrasil, 2018. Disponível em: https:/advpt.jusbrasil.com.br/artigos582641980/fake-news-o-direito-e-asprovidências. Acesso em: 17 de set. 2021.

Outro comum motivo é o comercial, as mídias moldam a realidade dos fatos para mostrar o que eles querem que os telespectadores vejam e, assim, atrair visualizações e, consequentemente, arrecadam com isso.

> O jornalismo como um todo, tem o propósito de nos apresentar os acontecimentos que surgem no mundo referencial. Mas o que faz realmente é entregar um mundo construído por ele mesmo. [...] Ele reflete o espaço social ao mesmo tempo que é refletido por ele. É nesse jogo, de oferece o que o público deseja de acordo com seus próprios interesses que o discurso midiático e jornalístico, em particular, começam a tomar forma[4].

Segundo o advogado especialista em Direito Digital e Cibercrimes, D´Urso, defende que existem duas principais características para justificar o motivo da força de uma notícia falsa, seria o viés de confirmação e o fato dessas notícias falsas serem compartilhadas por pessoas conhecidas.

> O viés de confirmação se dá quando a notícia falsa confirma uma opinião pré-existente e o indivíduo se sente tão satisfeito em estar certo, que compartilha sem verificar a procedência da notícia. Já em relação ao recebimento de notícias de conhecidos, que chegam por familiares, amigos etc., os filtros naturais de desconfiança acabam diminuindo, estimulando o compartilhamento sem prévia verificação[5] (D'URSO, 2018).

2.2 As estatísticas e suas consequências

Em um estudo realizado pela Avaaz[6] sobre notícias falsas sobre a pandemia, descobriu-se cerca de 110 milhões de brasileiros acreditam em pelo menos uma notícia falsa sobre o COVID. Ou seja, sete em cada dez brasileiros. O estudo aponta as maiores responsáveis por isso são as redes sociais, principalmente o WhatsApp e o Facebook.

Ao analisar o número da população brasileira com o número dos usuários ativos dessas redes temos que: a população brasileira atualmente é de 213,3 milhões

[4] MEDINA, Leonardo Cezar Correa**. Transgredindo o discurso jornalístico: A paródia nas reportagens de Ernesto Varela**. Dissertação (Mestrado) – Programa de Pós-Graduação em Estudos Linguísticos da Faculdade de Letras da Universidade Federal de Minas Gerais. 2012.

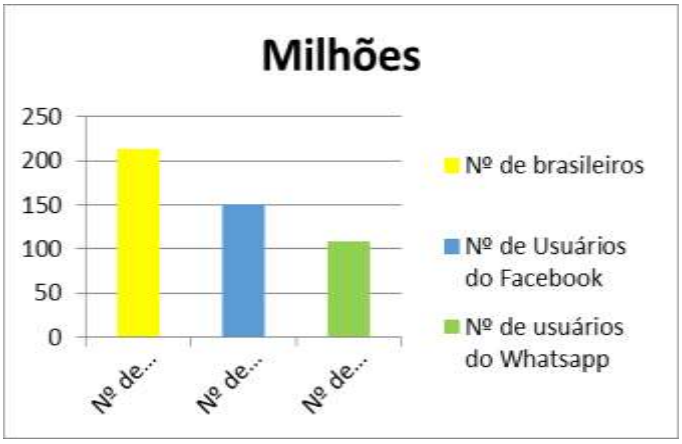
[5] D'URSO, Luiz Augusto Filizzola. **É crime compartilhar uma Fake News?** Canal Ciências Criminais, Porto Alegre, 2018. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/artigos/585697974/e-crime-compartilhar-uma-fake-news. Acesso em: 18 de set. 2021.

[6] Estado de Minas. **Coronavírus:** fake News atinge 110 milhões de brasileiros. Disponível em: <https://www.em.com.br/app/noticia/bem-viver/2020/05/21/interna_bem_viver,1149424/coronavirus-fake-news-atinge-110-milhoes-de-brasileiros.shtml> Postado em: 21/05/2020. Acesso em: 18 de set. 2021.

em 2021, segundo estimativa do Instituto Brasileiro de Geografia e Estatística[7]; o número de usuários do WhatsApp no Brasil é de 108,4 milhões segundo a Business Insides[8]; já o número de usuários do Facebook chega a marca de 150 milhões de brasileiros[9].

Vejamos isso no gráfico:

Gráfico 1 - Número de Brasileiros e números de usuários do Facebook e do WhatsApp



Verifica-se que a maioria da população brasileira se encontra conectada as mídias sociais. Questiona-se se os brasileiros sabem reconhecer se uma notícia é falsa ou não. Nessa mesma linha de raciocínio, um estudo realizado pela Kaspersky[10] apontou que 62% dos brasileiros não sabem distinguir se a notícia é falsa ou verdadeira. Mas 62% é até que considerado pouco, comparado aos peruanos (79%), em segundo lugar os colombianos (73%), em terceiro os chilenos (70%), mexicanos e argentinos empatam com 66% de pessoas que não conseguem identificar uma notícia falsa.

[7] Agência Brasil**. População brasileira chega a 213,3 milhões de pessoas em 2021**. Publicado em: 27/08/2021. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2021-08/populacao-brasileira-chega-2133-milhoes-de-pessoas-em-2021> Acessado em: 18 de set. 2021

[8] Affde. **Estatísticas do usuário do WhatsApp 2021: quantas pessoas usam o WhatsApp?** Publicado em: 22/07/2021. Disponível em: <https://www.affde.com/pt/whatsapp-users.html> Acesso em: 18 de set. 2021

[9] Hostmídia. **As 10 redes sociais mais usadas no Brasil em 2021**. Disponível em: <https://www.hostmidia.com.br/blog/redes-sociais-mais-usadas/> Acesso em: 18 de set. 2021

[10] Canaltech. **62% dos brasileiros não sabem reconhecer fake News, diz pesquisa.** Publicado em: 13/02/2020. Disponível em: <https://canaltech.com.br/seguranca/brasileiros-nao-sabem-reconhecer-fake-news-diz-pesquisa-160415/ Acesso em: 19 set. 2021

Um outro grande problema das notícias falsas é que elas se espalham 70% mais rápido do que as verdadeiras, segundo um estudo realizado por cientistas do Instituto de Tecnologia de Massachusetts, pulicado na revista Science[11]. Percebeu-se que as informações falsas atingem de mil a 100 mil pessoas, já as verdadeiras atingem, em média, mil pessoas.

Ainda sobre esse estudo, perceberam, também, que quando se trata de notícias falsas ligadas à política, elas atingem o público três vezes mais rápido do que uma simples notícia falsa. Eles defendem que os métodos para espalhar notícias falsas estão cada vez mais sofisticadas e que as empresas como Google, Facebook e Twitter são responsáveis eticamente e socialmente e deveriam contribuir para eliminar as notícias falsas.

Uma notícia falsa pode não parecer grande coisa, mas vejamos agora algumas consequências de uma informação falsa em casos reais.

Em São Paulo, no ano de 1994, teve um caso conhecido como ´´Caso Escola Base´´[12]. Onde a imprensa chamou os donos da escola, mais o motorista e uma professora de pedófilos, sem qualquer chance de defesa dos acusados. Não só isso, alegaram que as crianças eram drogadas, fotografadas sem roupas e que a Kombi usada para levar as crianças de casa para a escola e da escola para casa era usada como um motel.

A notícia se espalhou e a escola foi depredada pela população revoltada, tendo como consequência o fechamento dela. Não só a escola sofreu com isso como também as pessoas acusadas passaram a sofrer ameaças e adquiriram doenças como estresse, fobia e cardiopatia. Além disso, perderam seus empregos e precisaram se isolar da sociedade.

Após as investigações, descobriu-se que tudo se tratava de uma notícia falsa, não tendo qualquer prova contra os envolvidos. Posteriormente, a imprensa foi

[11] Correio Braziliense. **Fake news se espalham 70% mais rápido que notícias verdadeiras, diz MIT**. Publicado em: 08/03/2018. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/tecnologia/2018/03/08/interna_tecnologia,664835/fake-news-se-espalham-70-mais-rapido-que-noticias-verdadeiras.shtml> Acesso em: 19 set. 2021

[12] Pragmatismo político. **Caso Escola Base: Rede globo é condenada a pagar R$1,35 milhão**. Publicado em 17/12/2021. Disponível em: <https://www.pragmatismopolitico.com.br/2012/12/caso-escola-base-rede-globo-e-condenada-pagar-r-135-milhao.html> Acesso em: 20 de set 2021

condenada a pagar uma indenização de R$ 1,35 milhões[13] aos acusados. Entretanto, nenhuma indenização seria capaz de fazer com que eles perdessem as doenças já adquiridas e as outras consequências dessa notícia falsa.

A BBC fez uma matéria contando os três maiores casos de Fake News que acarretaram guerras e conflitos ao redor do mundo todo[14].

O primeiro caso, foi o do "menino crucificado na Ucrânia". A Ucrânia estava passando por um grave conflito interno e, em decorrência disso, perdeu parte de seu território para a Rússia. Acontecesse que a Rússia, para dar credibilidade a essa ocupação, divulgou notícias mostrando ucranianos crucificando crianças e que uma mãe teve que assistir seu filho sendo morto por eles. Consequentemente, isso favoreceu a opinião pública para que a Rússia ocupasse parte da Ucrânia. Entretanto, tempo depois, foi comprovado que tudo não passou de uma mentira.

O segundo caso, também chamado de ´´A menina do Kuwait e a invasão do Iraque´´, ocorreu em 1990, meses depois que o Iraque invadiu o Kuwait. Nesse momento, os Estados Unidos tinham fixado um prazo para que o exercite do Iraque se retirasse do Kuwait. A população americana estava dividida entre apoiar ou não essa intervenção. Para conseguir o apoio dos Estados Unidos, uma menina Kuaitiana falou, em um Congresso, que os soldados iraquianos estavam retirando os bebês prematuros das incubadoras para que morressem.

O impacto desse discurso foi tão grande que fez com que os Estados Unidos tivessem legitimação para participarem da guerra do Golfo. Entretanto, esse discurso era falso e a menina usada para falar esse discurso era filha do embaixador do Kuwait nos Estados Unidos.

O terceiro acontecimento contado nessa matéria da BBC foi o recente caso das fotos falsas na crise dos rohingya. Por conta da existência de uma perseguição no país de Myanmar, a população Rohingya não tinha direito a cidadania, não sendo

[13] Pragmatismo político. **Caso Escola Base: Rede globo é condenada a pagar R$1,35 milhão**. Publicado em 17/12/2021. Disponível em: <https://www.pragmatismopolitico.com.br/2012/12/caso-escola-base-rede-globo-e-condenada-pagar-r-135-milhao.html> Acesso em: 20 de set 2021

[14] BBC News. **Três casos de fake News que geraram guerras e conflitos ao redor do mundo.** Disponível em: <https://www.bbc.com/portuguese/geral-43895609> Acesso em: 20 set. 2021

considerados cidadãos, não existiam direitos básicos para eles e eram constantemente perseguidos.

Como uma forma de justificar essa perseguição, no ano de 2017, foram divulgadas fotos tiradas em antigos conflitos no ano de 1940 se passando como atuais para mostrar budistas assassinados por Rohingyas, para insinuar que eles seriam imigrantes ilegais e violentos. Por conta dessas fotos reais, mas fora de contexto, mais de 600 mil Rohingya tiveram que procurar refúgio em Bangladesh.

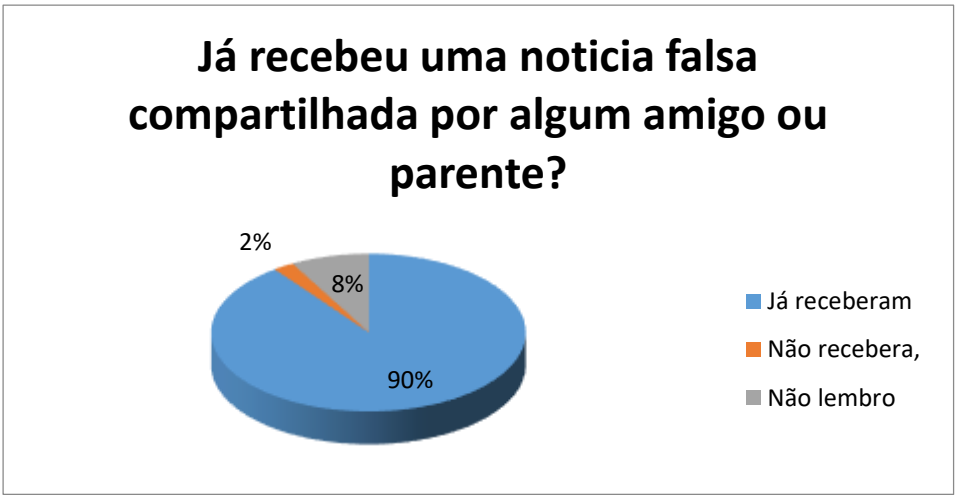
3 OPINIÃO PÚBLICA SOBRE A RESPONSABILIDADE DO USO DE FAKE NEWS OBSTÁCULOS

Com a ajuda de 186 pessoas, foi realizada uma rápida enquete[15] de cinco perguntas com o intuito de analisarmos a opinião delas referente a responsabilidades dos criadores, compartilhadores e provedores das mídias sociais, e como interagiram ao receberem uma notícia falsa.

A primeira pergunta foi para termos uma ideia de quantas pessoas já receberam notícias falsas compartilhadas por algum amigo ou parente. Obtivemos como resposta de que 167 pessoas já receberam notícias falsas de algum amigo o parente, 4 pessoas alegaram que não receberam e 15 pessoas não lembram se já receberam ou não.

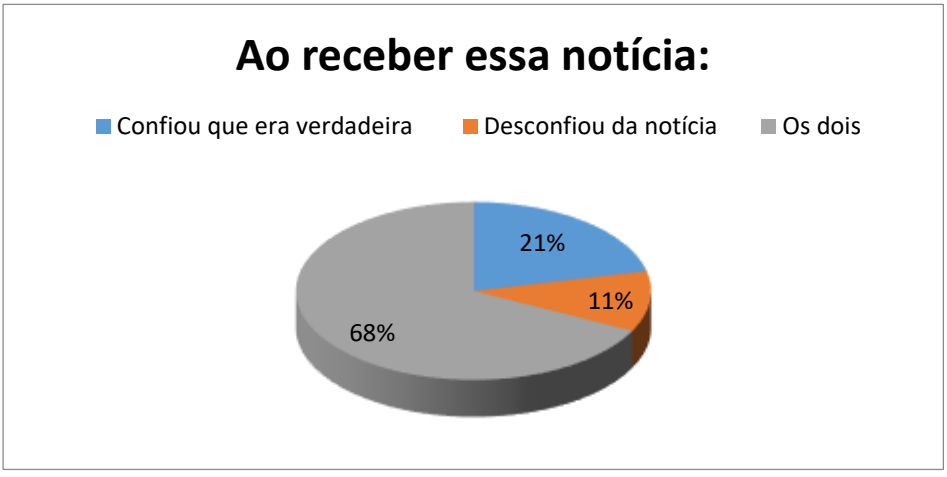
[15] A enquete foi realizada pelo Instagram do Autor, ficando disponível por 34 horas e obteve a participação de 186 pessoas, não sendo considerado, para a realização dessa enquete, a idade dos participantes.

Gráfico 2 - Primeira pergunta



A segunda pergunta teve o objetivo de analisarmos se essas pessoas que receberam essa notícia falsa de um parente ou amigo, confiou que era verdadeira, desconfiou da notícia ou se já ocorreram as duas coisas. Como resposta, obtivemos que 39 pessoas confiaram logo de cara que a notícia era verdadeira, 20 pessoas desconfiaram e que 123 pessoas já tiveram as duas experiências.

Gráfico 3 - Segunda pergunta

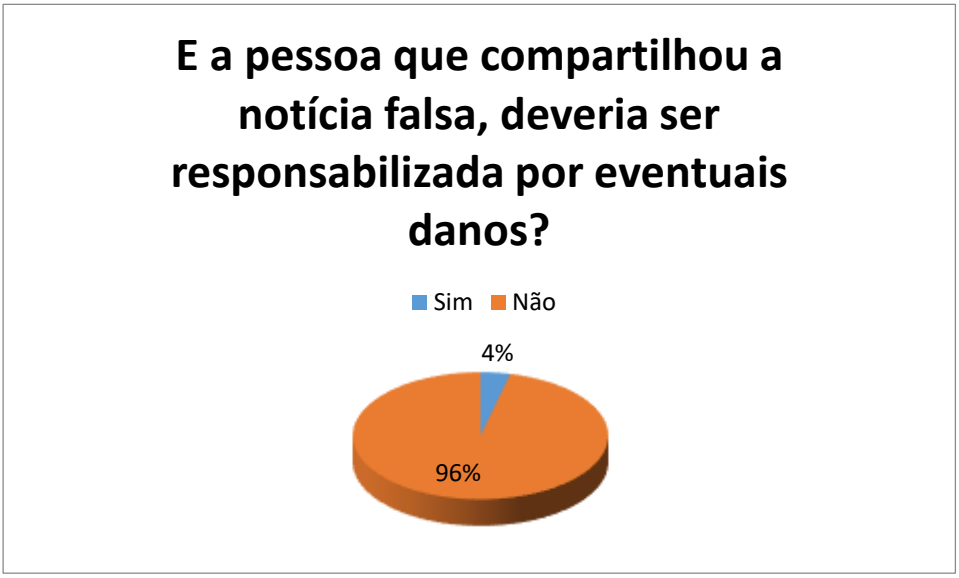


A terceira pergunta foi, com todos os participantes, se eles acreditam que a pessoas que criou a notícia falsa deveria ou não responder por eventuais danos. Como resposta, tivemos que 183 pessoas concordam que o criador da notícia deveria sim responder por eventuais danos e que 3 pessoas defendem que não deveriam responder.

Gráfico 4 - Terceira pergunta

A penúltima pergunta teve o intuito de descobrir se as pessoas que compartilham a notícias falsas deveriam ou não responder por eventuais danos. Obtivemos que 179 pessoas defendem que quem compartilha a notícia não deveria responder por eventuais danos e que 7 pessoas defender que deveriam responder sim por eventuais danos.

Gráfico 5 - Quarta pergunta



A última pergunta teve o objetivo de analisarmos qual seria a opinião delas sobre a responsabilidade das mídias sociais sobre eventuais danos causados por seus usuários. Como resultado percebe-se que 185 pessoas acreditam que as mídias sociais não teriam qualquer responsabilidade e 1 pessoa defende que teriam responsabilidade.

Gráfico 6 - Quinta pergunta

Ao analisar os gráficos dessa enquete, temos que o recebimento de notícias falsas tornaram-se algo normal de se acontecer. Além disso, demostra que a notícia, ao ser enviada por alguém de confiança, traz consigo uma veracidade. A consequência disso é a porcentagem existente das pessoas que não verificarão a autenticidade dessa notícia.

Já a responsabilidade, a maioria apoiaram pela responsabilidade exclusiva dos criadores das notícias falsas e não de quem a compartilha e das redes utilizadas para isso. Vejamos a seguir a responsabilidade em decorrência de notícias falsas no ordenamento jurídico.

3.1 Afinal, qual o crime e de quem é a responsabilidade?

Questiona-se qual seria, então, a posição do ordenamento jurídico qual seria o crime para quem compartilha uma notícia falsa e se os provedores seriam também responsáveis.

No ordenamento brasileiro, para quem cria e para quem compartilha a notícia falsa, precisaria se enquadrar nos crimes previstos no Capítulo V do Código Penal, sendo eles: Calúnia; difamação; e injúria.

> **Calúnia:** Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa. § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga. § 2º - É punível a calúnia contra os mortos.
>
> **Difamação:** Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa.
>
> **Injúria:** Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa. § 1º - O juiz pode deixar de aplicar a pena: I - quando o ofendido, de forma reprovável, provocou diretamente a injúria; II - no caso de retorsão imediata, que consista em outra injúria. § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes: Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência. § 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência. Pena - reclusão de um a três anos e multa.

Fora isso, pegando como exemplo noticiais falsas que foram divulgadas durante o covid no mundo todo, mencionado por um artigo da Uol[16], como: na índia, houve grande boatos de que a urina de uma vaca, animal sagrado na cultura indiana, seria um remédio eficaz contra o covid; na América Latina, foi repassado a informação de que termômetros infravermelhos, usados para medir a temperatura das pessoas em shoppings, mercados e outros, afetavam uma glândula pineal e acarretava na morte de neurônios; já na França, foi divulgado numa página sobre agricultura de que os consumidores de carne bovinas eram imunes ao vírus e que o vírus só se espalhou na China por conta que o consumo de carne lá era muito baixo; e muitos outros. Essas notícias, assim como muitas outras, não geram qualquer responsabilidade para quem a cria e para quem a compartilha.

[16] Uol. **Conheça as fake News mais absurdas já checadas sobre o coronavírus no mundo**. Publicado em: 31/08/2020. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/08/31/conheca-as-fake-news-mais-absurdas-ja-checadas-sobre-o-coronavirus.htm> Acesso em: 20 set. 2021

Já quanto aos provedores de internet, segundo entendimento do STJ, não teriam responsabilidade objetiva quanto à ofensa causada pelo seu usuário e nem seriam de sua responsabilidade a fiscalização dos conteúdos postados.

> AGRAVO INTERNO NO RECURSO ESPECIAL. AÇÃO INDENIZATÓRIA. DANOS MORAIS. RESPONSABILIDADE CIVIL DE PROVEDOR DE INTERNET. OFENSAS INSERIDAS POR ANÔNIMO NO SITE DE RELACIONAMENTOS ORKUT. RETIRADA DE CONTEÚDO OFENSIVO APÓS A NOTIFICAÇÃO. INEXISTÊNCIA DE ATO ILÍCITO. PRECEDENTES. AGRAVO NÃO PROVIDO. 1. A jurisprudência desta Corte caminha no sentido de que: I) o dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade desenvolvida pelo provedor de conteúdo, pelo que não se lhe é aplicável a responsabilidade objetiva, prevista no art. 927, parágrafo único, do CC/2002; II) a fiscalização prévia dos conteúdos postados não é atividade intrínseca ao serviço prestado pelo provedor de conteúdo [...][17].

Pinheiro argumenta que para falarmos de responsabilidade, deveríamos entender se a internet é um lugar ou um meio. Se considerarmos a internet como um lugar, logo deveríamos ter que redesenhar o Direito, já que a jurisdição e o território seriam a própria internet. Entretanto, se considerarmos a internet como um meio, assim como rádio, telefone, televisão, teríamos o desafio de aplicar as antigas normas ou atualizar normas para se adequar ao caso concreto simultaneamente com as mudanças da própria sociedade.

> Se entendermos que a Internet é um lugar, então muitas questões do Direito devem ser redesenhadas, uma vez que o território ou jurisdição deveria ser a própria Internet. Se entendermos que a Internet é um meio, então voltamos a ter de resolver a questão da territorialidade para a aplicação da norma, já havendo como referência a atuação do Direito Internacional. [...] Se a Internet é um meio, como é o rádio, a televisão, o fax, o telefone, então não há que falar em Direito de Internet, mas sim em um único Direito Digital cujo grande desafio é estar preparado para o desconhecido, seja aplicando antigas ou novas normas, mas com capacidade de interpretar a realidade social e adequar ao caso concreto na mesma velocidade das mudanças da sociedade[18].

[17] BRASIL. Superior Tribunal de Justiça, AgInt no REsp 1.507.782/RS, Rel. Min. Raul Araújo. DJ 03 mar. 2020. Disponível em: https://ww2.stj.jus.br/processo/pesquisa/?termo=resp1.507.782&aplicacao=processos.ea&tipoPesquisa=tipoPesq uisaGenerica&chkordem=DESC&chkMorto=MORTO. Acesso em: 20 set. 2021

[18] PINHEIRO, Patrícia Peck. **Direito digital.** 6. ed. São Paulo: Saraiva, 2016, p. 71.

Outro detalhe para ser observado é o que faz uma notícia ser considerada falsa, isso porque se formos pensar em uma notícia em que alega que determinada receita caseira é um remédio natural para alguma doença, mas que a ciência ainda não conseguiu comprovar tal alegação. Seria uma notícia falsa ou não? E se fosse considerada uma notícia falsa, mas, posteriormente, fosse comprovado ser realmente eficaz, o que aconteceria caso existisse a condenação da pessoa que criou essa receita e que comentou sobre seus benefícios?

Ademais, como no caso acima, quem decidiria se a notícia é falsa ou não? Pegando como exemplo o caso da cloroquina, muitos médicos e especialistas encontram-se em grande discordância, pois uns alegam que ela é sim um medicamento eficaz contra a COVID-19, já outros alegam que ela não é recomendada para o tratamento. Nesse caso, um médico que defende um ponto, mas que não foi comprovado, estaríamos diante de uma notícia falsa? E se, posteriormente, foi comprovado o oposto do que ele alega, teria alguma consequência?

Já uma notícia falsa divulgada por uma emissora, seria considerado um erro jornalístico ou seria considerado e tratada como uma Fake News?

4 CONSIDERAÇÕES FINAIS

Ao longo do artigo, percebeu-se que as notícias falsas possuem um alcance muito maior do que uma notícia verdadeira, principalmente se ela possui um viés político e que as consequências de sua criação são inúmeras, podendo até gerar guerras.

Não é de hoje que existem as Fake News, desde a história da nossa sociedade temos o conhecimento da existência de mentiras contadas. Trata-se de uma maneira de manchar a imagem de alguém, manipular uma opinião, vender uma notícia e muitos outros motivos que levariam alguém a criar uma notícia falsa.

O grande problema na notícia falsa está no alcance que ela chega e, principalmente, na dificuldade das pessoas saberem distinguir ou averiguar sua veracidade. Dessa forma, muitas notícias falsas acabam sendo passadas como verdadeiras e acarretam sérios danos. Dentre eles, como citado no artigo, o caso da

escola base, do menino crucificado na Ucrânia, o caso da menina do Kuwait que acabou acarretando na invasão do Iraque e muitos outros.

Na opinião pública, a responsabilidade por uma notícia falsa estaria apenas no criador dela e quem compartilha não teria qualquer responsabilidade por eventuais danos. Da mesma forma que as mídias também não teriam qualquer responsabilidade pelo que seus usuários escrevem.

Por fim, percebeu-se que o ordenamento jurídico expõe que só seriam responsáveis por eventuais danos se ocorresse o enquadramento nos crimes de calúnia, difamação e injúria. Caso não fosse enquadrado, a pessoa que criou e nem a pessoa que compartilhou, não teriam qualquer responsabilidade.

Por mais que esteja já no costume da humanidade a mentira, que seja algo considerado comum, o ordenamento jurídico não se adequou para acompanhar a evolução da informação de uma forma totalmente eficaz, deixando, assim, várias lacunas e perguntas a serem respondidas.

REFERÊNCIAS

Affde. **Estatísticas do usuário do WhatsApp 2021: quantas pessoas usam o WhatsApp?** Publicado em: 22/07/2021. Disponível em: <https://www.affde.com/pt/whatsapp-users.html>

Agência Brasil**. População brasileira chega a 213,3 milhões de pessoas em 2021**. Publicado em: 27/08/2021. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2021-08/populacao-brasileira-chega-2133-milhoes-de-pessoas-em-2021>

BBC News. **Três casos de fake News que geraram guerras e conflitos ao redor do mundo.** Publicado em: 25/04/2018 disponível em: <https://www.bbc.com/portuguese/geral-43895609>

BRASIL. Superior Tribunal de Justiça, AgInt no REsp 1.507.782/RS, Rel. Min. Raul Araújo. DJ 03 mar. 2020. Disponível em: <https://ww2.stj.jus.br/processo/pesquisa/?termo=resp1.507.782&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&chkordem=DESC&chkMorto=MORTO>.

Canaltech. **62% dos brasileiros não sabem reconhecer fake News, diz pesquisa.** Publicado em: 13/02/2020. Disponível em:

https://canaltech.com.br/seguranca/brasileiros-nao-sabem-reconhecer-fake-news-diz-pesquisa-160415/>

CASTRO, Paulo Tiago de. **Fake News, o Direito e as Providências**. Jusbrasil, 2018. Disponível em: <https:/advpt.jusbrasil.com.br/artigos582641980/fake-news-o-direito-e-asprovidências>.

Correio Braziliense. **Fake news se espalham 70% mais rápido que notícias verdadeiras, diz MIT**. Publicado em: 08/03/2018. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/tecnologia/2018/03/08/interna_tecnologia,664835/fake-news-se-espalham-70-mais-rapido-que-noticias-verdadeiras.shtml>

D'URSO, Luiz Augusto Filizzola. **É crime compartilhar uma Fake News?** Canal Ciências Criminais, Porto Alegre, 2018. Disponível em: <https://canalcienciascriminais.jusbrasil.com. br/artigos/585697974/e-crime-compartilhar-uma-fake-news>.

Estado de Minas. **Coronavírus:** fake news atinge 110 milhões de brasileiros. Postado em: 21/05/2020. Disponível em: <https://www.em.com.br/app/noticia/bem-viver/2020/05/21/interna_bem_viver,1149424/coronavirus-fake-news-atinge-110-milhoes-de-brasileiros.shtml>

Hostmídia. **As 10 redes sociais mais usadas no Brasil em 2021**. Disponível em: <https://www.hostmidia.com.br/blog/redes-sociais-mais-usadas/>

MEDINA, Leonardo Cezar Correa**. Transgredindo o discurso jornalístico: A paródia nas reportagens de Ernesto Varela**. Dissertação (Mestrado) – Programa de Pós-Graduação em Estudos Linguísticos da Faculdade de Letras da Universidade Federal de Minas Gerais. 2012.

PINHEIRO, Patrícia Peck. **Direito digital.** 6. ed. São Paulo: Saraiva, 2016.

Pragmatismo político. **Caso Escola Base: Rede globo é condenada a pagar R$1,35 milhão**. Publicado em 17/12/2021. Disponível em: <https://www.pragmatismopolitico.com.br/2012/12/caso-escola-base-rede-globo-e-condenada-pagar-r-135-milhao.html>

Significados. **Fake News**. Disponível em: <https://www.significados.com.br/fake-news/>

Uol. **Conheça as fake News mais absurdas já checadas sobre o coronavírus no mundo**. Publicado em: 31/08/2020. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/08/31/conheca-as-fake-news-mais-absurdas-ja-checadas-sobre-o-coronavirus.htm>

A LIBERDADE DE EXPRESSÃO COMO UM DIREITO FUNDAMENTAL E A INTERNET: QUANDO A LIBERDADE DE EXPRESSÃO INDIVIDUAL CONFRONTA UM OUTRO DIREITO INDIVIDUAL

Gabriella Navarro de Azevedo Pinheiro[1]

RESUMO

O presente trabalho visa introduzir uma breve discussão acerca da liberdade de expressão como direito fundamental e o avanço da tecnologia nos meios de comunicação: a era da Internet. A Constituição Federal Brasileira de 1988 garante a liberdade de expressão como um direito fundamental, vedando o anonimato, ou seja, o autor da manifestação, e nesse caso, seja ela feita no formato que for, tem o dever de se identificar e as pessoas que estão lendo a referida manifestação têm o direito de saber quem a escreveu. Com o avanço da comunicação por meios tecnológicos, houve uma necessidade urgente de uma legislação específica para os agentes desse processo da rede de internet, afinal, um espaço de ideias, informações, precisa coexistir com regras, assim como todos os setores da sociedade. Nesse sentido em 2014 a Lei 12.965, denominada Marco Civil da Internet, foi sancionada com o escopo principal de regulamentar as relações no ambiente da internet, estabelecendo princípios, garantias e deveres aos agentes envolvidos. E a liberdade de expressão, como uma garantia fundamental, é um direito absoluto ou coexiste proporcionalmente com as outras garantias e o seu excesso, caso provoque danos, é passível de responsabilização? O indivíduo que ao exercer o seu direito de liberdade de expressão, desrespeita uma outra garantia constitucional do outro, pode ser responsabilizado? E sendo responsabilizado, esse fato mitiga o direito de liberdade de expressão, ou apenas responsabiliza alguém por excesso cometido no exercício de sua liberdade? O A legislação pertinente e específica para essas relações virtuais possui muitas lacunas ainda, mas considerando-se a velocidade da realidade tecnológica, o Direito não consegue acompanhar paralelamente o referido avanço. Dessa forma, há situações em que o Marco Civil da Internet, assim como a Lei Geral de Proteção de Dados, terá que ser aplicado concomitantemente com a legislação não específica, que no Brasil é bastante consistente e robusta. Caso contrário, a

[1] Gabriella Navarro de Azevedo Pinheiro. Advogada inscrita sob a OAB DF 31.513, graduada pelo Centro Universitário de Brasília, e-mail: gabriellanapinheiro@gmail,com. Aluna do curso de pós-graduação lato sensu – Direito do Trabalho e Previdenciário - do Centro Universitário de Brasília– UniCEUB/ICPD.

atividade legislativa no sentido da criação e aprovação de leis teria que ser diária. Dessa forma, o Marco Civil da Internet foi um avanço significativo no sentido mais relevante de proteção dos direitos fundamentais previstos na CF de 1988, de todos os agentes das relações virtuais. E nesse sentido a liberdade de expressão reflete um importante pilar e uma garantia fundamental.

Palavras-chave: Liberdade de Expressão. Internet. Limites.

ABSTRACT

This paper aims to introduce a brief discussion about freedom of expression as a fundamental right and the advancement of technology in the media: the Internet era. The Brazilian Federal Constitution of 1988 guarantees freedom of expression as a fundamental right, prohibiting anonymity, that is, the author of the manifestation, and in this case, regardless of the format, it has the duty to identify itself and the people who are reading the above demonstration have the right to know who wrote it. With the advancement of communication by technological means, there was an urgent need for specific legislation for the agents of this internet network process, after all, a space of ideas, information, needs to coexist with rules, as well as all sectors of society. In this sense, in 2014, Law 12.965, known as the Marco Civil da Internet, was enacted with the main scope of regulating relationships in the internet environment, establishing principles, guarantees and duties for the agents involved. And is freedom of expression, as a fundamental guarantee, an absolute right or does it coexist proportionally with the other guarantees and is its excess, if it causes damage, liable to liability? Can the individual who, by exercising his right to freedom of expression, disrespect another constitutional guarantee be held liable? And being held responsible, does this fact mitigate the right to freedom of expression, or does it just hold someone responsible for the excess committed in the exercise of their freedom? The pertinent and specific legislation for these virtual relationships still has many gaps, but considering the speed of technological reality, the Law cannot accompany the referred advance in parallel. Thus, there are situations in which the Marco Civil da Internet, as well as the General Data Protection Law, will have to be applied concurrently with non-specific legislation, which in Brazil is quite consistent and robust. Otherwise, the legislative activity towards the creation and approval of laws would have to be daily. In this way, the Marco Civil da Internet was a significant advance in the most relevant sense of protection of the fundamental rights provided for in the Federal Constitution of 1988, of all agents of virtual relations. And in this sense, freedom of expression reflects an important pillar and a fundamental guarantee.

Keywords: Freedom of expression. Internet. Limits.

1 INTRODUÇÃO

A liberdade é uma conquista histórica da humanidade, e nos tempos atuais é inimaginável, a aceitação do seu cerceamento, seja qual for o tema de fundo, nas sociedades democráticas.

O Direito à liberdade de expressão garante ao indivíduo como ator social, o direito fundamental a manifestar-se sobre qualquer assunto ou circunstância, expondo seus valores, pontos de vista, concepções. E essa é a forma mais verdadeira do exercício da cidadania.

No Brasil, a liberdade de expressão tem previsão legal na Constituição Brasileira de 1988, no art. 5º, e representa um dos principais pilares da Lei nº 12.965/2014, o Marco Civil da Internet.

O Marco Civil da Internet foi elaborado com o objetivo precípuo de regulamentar as relações no ambiente virtual da internet, estabelecendo princípios, garantias e deveres aos agentes envolvidos.

E como fica a liberdade de expressão nos ambientes virtuais? A liberdade de expressão de um indivíduo pode causar danos e desrespeitar algum tipo de direito de outra pessoa?

A Constituição Federal do Brasil de 1988, dispõe sobre a liberdade de expressão, vedando expressamente o anonimato. Isso quer dizer que a pessoa tem o direito de expressar livremente o que ela deseja, sem censura prévia, e segundo as suas opiniões, mas tem o dever de se identificar. E essa identificação tem a ver com as responsabilizações no caso da manifestação de uma pessoa, desrespeitar os direitos do outro.

O direito à liberdade de expressão coexiste com outros direitos como o direito à dignidade, à honra, e tantos outros. Apesar de direitos, é preciso que as os cidadãos não se distanciem das regras de convivência em sociedade, que implica em respeitar o direito do outro também. Nessa linha de raciocínio, poderia afirmar que até mesmo quando ao indivíduo é garantido um direito, essa garantia, impõe a ele o dever de no exercício desse direito, respeitar os direitos dos outros. Porque a sociedade é constituída por indivíduos com diversas garantias protegidas pelo ordenamento jurídico.

Nesse sentido, e com o imenso avanço dos meios de comunicação virtuais, faz-se necessária a análise da existência ou não de limites à liberdade de expressão. É certo que a Constituição Federal não dispõe sobre o cerceamento desse direito,

mas veda o anonimato e garante vários outros direitos aos cidadãos, que coexistem com a liberdade de expressão.

O presente trabalho faz uma análise desse contexto e o que existe em termos de legislação no Brasil, que possa dirimir as dúvidas sobre as limitações à liberdade de expressão e se esse direito se configuraria como algo que se se sobrepõe às outras garantias constitucionais.

2 A LIBERDADE DE EXPRESSÃO

A existência na esfera legal da liberdade de expressão consiste numa conquista de toda a humanidade e por isso faz parte de legislações da Organização das Nações Unidas, convenções internacionais e do regramento jurídico da maior parte dos países democráticos.[2]

A liberdade de expressão consiste no direito à livre manifestação, e em sentido mais amplo, reflete a proteção jurídica do espaço social para que cada indivíduo tenha a liberdade de expressar as suas opiniões e posições acerca de matérias diversas, baseando-se nos seus valores acumulados ao longo de sua vida, suas crenças e concepções.[3]

Desmembrando o sentido das duas palavras que compõem esse direito que é garantia constitucional no Brasil, tem-se a liberdade e a expressão.

Expressar significa fazer a revelação de uma opinião, uma concepção, um sentido sobre algo. As pessoas se expressam de maneira espontânea sobre algo irrelevante, assim como se expressam de forma articulada sobre tema relevante, socialmente falando, com o objetivo de formar opinião e demarcar posições na sociedade. E isso pode ser feito de diversas formas como em conversas, textos, seja de forma física quanto por meios tecnológicos, e dessa forma há a transmissão de uma mensagem com conceitos, opiniões, análises, críticas, sobre algo.[4]

[2] FIA, Fundação Instituto de Administração, 22 de set. de 2020. Liberdade de expressão: lei, evolução, importância e limites. Disponível em <https://fia.com.br/blog/liberdade-de-expressao/ > Acesso em 30 de set de 2021.

[3] BOTTI, Flávia. Principais aspectos jurídicos da liberdade de expressão. 2021. Disponível em < https://www.aurum.com.br/blog/liberdade-de-expressao/> Acesso em 29 de set, 2021.

[4] BOTTI, Flávia. Principais aspectos jurídicos da liberdade de expressão. 2021. Disponível em < https://www.aurum.com.br/blog/liberdade-de-expressao/> Acesso em 29 de set, 2021.

A liberdade de expressão é antes e tudo uma espécie de direito natural do ser humano. Isso porque o indivíduo nasce com uma condição humana, originária, de liberdade.[5]

Entretanto, para que uma garantia apesar de intrínseca ao ser humano, seja resguardada e respeitada, faz-se necessária a tutela pelo ordenamento jurídico. Assim, a Constituição Federal brasileira de 1988 assegura a liberdade de expressão como um direito fundamental:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:[6]
>
> (...)
>
> II – Ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;
>
> IV – é livre a manifestação do pensamento, sendo vedado o anonimato;
>
> V – É assegurado o **direito de resposta,** proporcional ao agravo, além da indenização por dano material, moral ou à imagem;
>
> VI – é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias;
>
> IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
>
> XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

No Art. 200, a lei reitera a liberdade de expressão:[7]

> "A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não

[5] BOTTI, Flávia. Principais aspectos jurídicos da liberdade de expressão. 2021. Disponível em < https://www.aurum.com.br/blog/liberdade-de-expressao/> Acesso em 29 de set, 2021.

[6] BRASIL. Constituição (1988). Constituição da República Federativa do Brasil: texto constitucional promulgado em 5 de outubro de 1988, compilado até a Emenda Constitucional nº 109/2021. – Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2021. 426p.

[7] BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil: texto constitucional promulgado em 5 de outubro de 1988, compilado até a Emenda Constitucional nº 109/2021.* – Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2021. 426p.

> sofrerão qualquer restrição, observado o disposto nesta constituição."
>
> "É vedada toda e qualquer censura de natureza política, ideológica e artística."

O Pacto Internacional dos Direitos Civis e Políticos teve a sua adoção feita pela Resolução n. 2.200-A da Assembleia Geral das Nações Unidas, em dezembro de 1966. Dessa forma, o alcance do pacto passou a ser mundial, entrando em vigência em 1976.[8]

O Congresso Brasileiro aprovou o pacto por meio do Decreto Legislativo 226, de 1991, a carta de adesão do Brasil foi depositada em 1992, e entrou em vigência ainda nesse ano, por meio do Decreto 592 que em seu artigo 19, preceitua:

> Art. 19 – Toda pessoa terá direito à liberdade de expressão; esse direito incluirá a liberdade de procurar, receber, e difundir informações e ideias de qualquer natureza, independentemente de considerações de fronteiras, verbalmente ou por escrito, em forma impressa ou artística, ou por qualquer outro meio de sua escolha[9]

Dessa forma, verifica-se que no Brasil, a Constituição de 1988 dispõe sobre garantias legais tanto de comunicações, quanto intelectuais e religiosas que servem de proteção à difusão e exposição de ideias pelos indivíduos que possuem a liberdade de expressar-se segundo suas opiniões, valores e concepções.

A liberdade de expressão pode ser entendida como o direito que o indivíduo tem de expressar as suas opiniões, ideias e críticas, de diversas formas, como discursos e textos escritos. Dessa forma, constitui-se assim, um importante instrumento para o exercício da democracia, no sentido mais amplo da cidadania.[10]

3 A LEI Nº 12.965/2014: O MARCO CIVIL DA INTERNET

A tecnologia da informação desde o final do século XX vem se transformando em algo acessível e com um alcance relevante, em decorrência do

[8] BRASIL, Decreto 592 de 06 de julho de 1992. Dispõe sobre Atos internacionais. Pacto Internacional sobre direitos civis e políticos. Promulgação. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm > Acesso em 30 de set. 2021.

[9] BRASIL, Decreto 592 de 06 de julho de 1992. Dispõe sobre Atos internacionais. Pacto Internacional sobre direitos civis e políticos. Promulgação. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm > Acesso em 30 de set. 2021.

[10] Disponível em: <https://www.migalhas.com.br/coluna/constituicao-na-escola/287487/liberdade-de-expressao-em-tempos-de-internet > Acesso em 29 de set, 2021, 19:35.

aspecto prático da comunicação digital, a utilização de computadores e outras ferramentas eletrônicas na realização de tarefas como o envio de informações entre indivíduos em locais distantes do planeta, entre várias atividades existentes, num espaço de segundos.[11]

Com esse crescimento exponencial da utilização das redes de internet surgiram vários tipos de questionamentos acerca das práticas de utilização desse meio tecnológico.

Tanto no Brasil, quanto em todo o mundo, a universalização do uso da internet implicou na necessidade da criação de regras de uso e convivência, e isso principalmente por se tratar de uma espécie de comunicação com caraterísticas bem próprias e específicas e que guardam correspondência entre si.[12]

As principais características supracitadas são a rapidez, a integração e a insegurança. A rapidez diz respeito à velocidade de transmissão de dados e informações, que se multiplicam aceleradamente e sem controle. A integração diz respeito ao caráter agregador de pessoas distintas que se comunicam ao mesmo tempo, falando coisas diferentes e propagando ideias e interpretações diversas de forma ampla e acelerada. Ainda, a insegurança, ocasionada pela aparente distância física que cria a impressão fictícia da impunidade, como se aquele espaço absolutamente privado estivesse longe da esfera jurídica do estado, e dessa forma não existissem regras e organização.[13]

Dessa forma, torna-se importante ressaltar que a pouco tempo atrás não existia no ordenamento jurídico do Brasil, nenhuma norma que regulamentasse ou estabelecesse limites aos inúmeros modelos de fluxo e acessos aos dados, nessa atividade de acesso à internet, no sentido amplo. Os usuários possuíam como

[11] XXXXXXXXXX

[12] AQUINO, Nick Richard. Antinomia jurídica entre o Marco Civil da Internet e o código de Defesa do Consumidor em matéria de Responsabilidade Civil dos provedores de aplicação de internet. Set. de 2015. Disponível em:< https://jus.com.br/artigos/42861/antinomia-juridica-entre-o-marco-civil-da-internet-e-o-codigo-de-defesa-do-consumidor-em-materia-de-responsabilidade-civil-dos-provedores-de-aplicacoes-de-internet> Acesso em 30 de set, 2021.

[13] AQUINO, Nick Richard. Antinomia jurídica entre o Marco Civil da Internet e o código de Defesa do Consumidor em matéria de Responsabilidade Civil dos provedores de aplicação de internet. Set. de 2015. Disponível em:< https://jus.com.br/artigos/42861/antinomia-juridica-entre-o-marco-civil-da-internet-e-o-codigo-de-defesa-do-consumidor-em-materia-de-responsabilidade-civil-dos-provedores-de-aplicacoes-de-internet> Acesso em 30 de set, 2021.

proteção legal, para o caso de ilegalidades e desrespeitos, o Código Civil e o Código de Defesa do Consumidor[14]

Assim diante das práticas novas de ilicitude e a ampliação meteórica da quantidade de usuários da rede, o Estado percebeu a clara necessidade da elaboração de legislação específica para as práticas on line para estabelecer regras, direitos, que não confrontem as garantias constitucionais que são conquistas da construção de uma sociedade democrática.[15]

O Marco Civil surgiu na verdade como a expectativa de dirimir dúvidas, construir acertos. Essa lei surgiu primeiramente com o objetivo de trazer clareza quanto a questão da responsabilidade dos provedores de internet, e ao fazer isso acabou por dispor sobre outros temas relevantes como a liberdade de expressão, bloqueio e retirada de informações ofensivas acerca dos indivíduos, direito à privacidade e outros.[16]

A Lei nº 12.965 é uma legislação ordinária federal, de iniciativa do Poder Executivo e reflete uma espécie de "Constituição da Internet".[17]

Conhecida como Constituição da Internet Brasileira, a referida lei tem por objetivo principal a disciplina da relação entre empresas operadoras de produtos ou serviços associados no ambiente da internet e os seus respectivos usuários dentro do território nacional.[18]

---

[14] AQUINO, Nick Richard. Antinomia jurídica entre o Marco Civil da Internet e o código de Defesa do Consumidor em matéria de Responsabilidade Civil dos provedores de aplicação de internet. Set. de 2015. Disponível em:< https://jus.com.br/artigos/42861/antinomia-juridica-entre-o-marco-civil-da-internet-e-o-codigo-de-defesa-do-consumidor-em-materia-de-responsabilidade-civil-dos-provedores-de-aplicacoes-de-internet> Acesso em 30 de set, 2021.

[15] AQUINO, Nick Richard. Antinomia jurídica entre o Marco Civil da Internet e o código de Defesa do Consumidor em matéria de Responsabilidade Civil dos provedores de aplicação de internet. Set. de 2015. Disponível em:< https://jus.com.br/artigos/42861/antinomia-juridica-entre-o-marco-civil-da-internet-e-o-codigo-de-defesa-do-consumidor-em-materia-de-responsabilidade-civil-dos-provedores-de-aplicacoes-de-internet> Acesso em 30 de set, 2021.

[16] AQUINO, Nick Richard. Antinomia jurídica entre o Marco Civil da Internet e o código de Defesa do Consumidor em matéria de Responsabilidade Civil dos provedores de aplicação de internet. Set. de 2015. Disponível em:< https://jus.com.br/artigos/42861/antinomia-juridica-entre-o-marco-civil-da-internet-e-o-codigo-de-defesa-do-consumidor-em-materia-de-responsabilidade-civil-dos-provedores-de-aplicacoes-de-internet> Acesso em 30 de set, 2021.

[17]RAMOS, Rahellen. O que é o Marco Civil da Internet? 06 de agosto de 2021. Disponível em:< https://www.politize.com.br/marco-civil-da-internet/ > Acesso em 29 de set, 2021.

[18] AQUINO, Nick Richard. Antinomia jurídica entre o Marco Civil da Internet e o código de Defesa do Consumidor em matéria de Responsabilidade Civil dos provedores de aplicação de internet. Set. de 2015. Disponível em:< https://jus.com.br/artigos/42861/antinomia-juridica-entre-o-marco-civil-da-

Trata-se de uma legislação de caráter principiológico, que possui como objetivo precípuo definir as garantias, os princípios, direitos e deveres que permeiam o uso da internet no país. E nesse sentido o Marco Civil da Internet teve o papel de instituir várias diretrizes que deverão ser seguidas pela União, estados, Distrito Federal e Municípios, provedores de internet, empresas e todos os agentes envolvidos nesse contexto virtual e tecnológico.[19]

O Marco Civil dispõe sobre regras e princípios que regerão todo processo de aplicação da internet, no qual os indivíduos que utilizam a rede passam a ser protagonistas. Sendo assim, essa lei tem como principal objetivo a garantia da dignidade dos indivíduos em termos de experiência nesse ambiente virtual.[20]

Muitos princípios e fundamentos fazem referência a questões já previstas em outros dispositivos do ordenamento jurídico brasileiro, como o direito à privacidade, o Direito à liberdade de expressão, o direito à dignidade. Por outro lado, questões novas surgiram nessa lei como a proposta de universalização do acesso à internet, como algo que faz parte do próprio exercício de cidadania do indivíduo.[21]

A Lei nº 12.965 tem sua fundamentação nos seguintes princípios: a liberdade de expressão, a neutralidade de rede e a privacidade.

A liberdade de expressão, tema do presente trabalho, em seu dispositivo constitucional, do art. 5º, veda o anonimato, e isso quer dizer que o direito à liberdade de expressão na CF de 1988 não tem um caráter absoluto, na medida em que aquele que se exceder no gozo do referido direito, poderá ser responsabilizado cível ou criminalmente.[22]

A neutralidade de rede que está prevista no art. 9 do Marco Civil dispõe que os provedores de internet têm o dever de tratar os pacotes de dados que transitam nas

internet-e-o-codigo-de-defesa-do-consumidor-em-materia-de-responsabilidade-civil-dos-provedores-de-aplicacoes-de-internet> Acesso em 30 de set, 2021.

[19]RAMOS, Rahellen. O que é o Marco Civil da Internet? 06 de agosto de 2021. Disponível em:< https://www.politize.com.br/marco-civil-da-internet/ > Acesso em 29 de set, 2021, 22:21.

[20]RAMOS, Rahellen. O que é o Marco Civil da Internet? 06 de agosto de 2021. Disponível em:< https://www.politize.com.br/marco-civil-da-internet/ > Acesso em 29 de set, 2021, 22:21.

[21]RAMOS, Rahellen. O que é o Marco Civil da Internet? 06 de agosto de 2021. Disponível em:< https://www.politize.com.br/marco-civil-da-internet/ > Acesso em 29 de set, 2021, 22:21.

[22]RAMOS, Rahellen. O que é o Marco Civil da Internet? 06 de agosto de 2021. Disponível em:< https://www.politize.com.br/marco-civil-da-internet/ > Acesso em 29 de set, 2021, 22:21.

respectivas redes, de forma isonômica, sem nenhum tipo de distinção em relação a conteúdos, aplicações, destinos, origem.[23]

O princípio supracitado foi o que causou maior polêmica durante as discussões acerca do projeto de lei. Isso porque o usuário pode acessar qualquer conteúdo na internet sem que os provedores possam fazer alguma intervenção ou interferência.

E ainda a privacidade, que também tem previsão no art. 5º da Constituição Federal de 1988, e na Lei 12.965/2014 esse direito tem o escopo de proteção dos dados dos usuários, com a exigência do consentimento expresso e ainda faz a previsão de indenizações em caso de violações à intimidade, vida privada dos indivíduos e comunicações sigilosas.[24]

A Lei 12.965 introduziu mudanças que acabaram por provocar relevantes impactos diretamente nos chamados procedimentos de transferência de informações dos usuários da rede de internet, e ainda a segurança que experimentam, durante o uso do meio tecnológico em questão.[25]

A partir da entrada em vigor do Marco Civil da Internet, em 23 de abril de 2014, muito além de estarem cientes sobre o tratamento conferido pelas empresas envolvidas nesse processo aos seus dados pessoais, o consentimento dos referidos usuários passa a ter expressão de forma obrigatória.[26]

Quando a lei foi sancionada, as empresas que dependem do uso de dados de navegação para executarem a execução de suas atividades, como por exemplo a

[23]RAMOS, Rahellen. O que é o Marco Civil da Internet? 06 de agosto de 2021. Disponível em:< https://www.politize.com.br/marco-civil-da-internet/ > Acesso em 29 de set, 2021, 22:21.

[24]RAMOS, Rahellen. O que é o Marco Civil da Internet? 06 de agosto de 2021. Disponível em:< https://www.politize.com.br/marco-civil-da-internet/ > Acesso em 29 de set, 2021, 22:21.

[25] FERREIRA, Fillipe. A proteção ao consumidor como direito fundamental constitucional: as garantias consumeristas. 01 de maio de 2018.Disponível em:<-https://ambitojuridico.com.br/edicoes/revista-172/a-protecao-ao-consumidor-como-direito-fundamental-constitucional-as-garantias-consumeristas/ > Acesso em 30 de set, 2021, 19:45.

[26]. FERREIRA, Fillipe. A proteção ao consumidor como direito fundamental constitucional: as garantias consumeristas. 01 de maio de 2018.Disponível em:<-https://ambitojuridico.com.br/edicoes/revista-172/a-protecao-ao-consumidor-como-direito-fundamental-constitucional-as-garantias-consumeristas/ > Acesso em 30 de set, 2021, 19:45.

Google e o Facebook foram as que mais sofreram o impacto das exigências normativas, a partir de então.[27]

Na verdade, o surgimento da internet e de empreendimentos eletrônicos acabou por ressaltar e renovar a grande relevância dos direitos fundamentais, a exemplos da autodeterminação informativa, a prerrogativa de controle da publicidade das próprias informações pessoais, que guardam relação direta com o direito à privacidade e à intimidade.[28]

E embora há inúmeras situações não elencadas ou com disposições claras e elencadas no Marco Civil da Internet, a referida lei significou um enorme avanço no sentido da regulamentação do ambiente virtual em todos os setores das relações estabelecidas no ambiente tecnológico, desde a garantia aos direitos fundamentais dispostos na Constituição Federal de 1988, os direitos consumeristas devido ao crescente comércio eletrônico, até a proteção dos dados cuidando do tratamento e circulação de informações que são dos indivíduos e não públicas. [29]

Em relação à proteção dos dados inclusive, em 2018 foi sancionada a Lei nº 13.709 – a LGPD, Lei Geral de Proteção de Dados. Essa lei representou mais um grande avanço na regulamentação das relações de consumo por meio do comércio eletrônico, com ascensão meteórica, acirrada ainda mais nesse período da crise de saúde provocada pela pandemia do novo Coronavírus, que assolou o mundo desde dezembro de 2019.[30]

A lei supracitada possui como escopo principal, a criação de um cenário juridicamente seguro, com a implementação de normas e práticas padronizadas para

---

[27]. FERREIRA, Fillipe. A proteção ao consumidor como direito fundamental constitucional: as garantias consumeristas. 01 de maio de 2018.Disponível em:<-https://ambitojuridico.com.br/edicoes/revista-172/a-protecao-ao-consumidor-como-direito-fundamental-constitucional-as-garantias-consumeristas/ > Acesso em 30 de set, 2021, 19:45.

[28]. FERREIRA, Fillipe. A proteção ao consumidor como direito fundamental constitucional: as garantias consumeristas. 01 de maio de 2018.Disponível em:<-https://ambitojuridico.com.br/edicoes/revista-172/a-protecao-ao-consumidor-como-direito-fundamental-constitucional-as-garantias-consumeristas/ > Acesso em 30 de set, 2021, 19:45.

[29] FERREIRA, Fillipe. A proteção ao consumidor como direito fundamental constitucional: as garantias consumeristas. 01 de maio de 2018.Disponível em:<-https://ambitojuridico.com.br/edicoes/revista-172/a-protecao-ao-consumidor-como-direito-fundamental-constitucional-as-garantias-consumeristas/ > Acesso em 30 de set, 2021, 19:45.

[30] BRASIL. Lei 13.709, de 13 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >Acesso em 01 de out, 2021, 14:27.

que os dados pessoais dos usuários que estiverem no Brasil sejam protegidos, dentro e fora do país de maneira correspondente, definindo em seu texto de forma clara o que são dados pessoais, aqueles que demandam cuidados específicos por serem sensíveis, para que a aplicabilidade da lei seja efetiva no sentido de restar claro quais deles estão sujeitos à regulação.[31]

Dessa forma, resta evidenciada a evolução da legislação brasileira no sentido dessa nova realidade que se impôs com a evolução das tecnologias e meios de comunicação e várias outras atividades que fazem parte do dia a dia da sociedade como um todo.

4 LIBERDADE DE EXPRESSÃO E INTERNET: HÁ LIMITES PARA A LIBERDADE DE EXPRESSÃO?

No vasto universo da liberdade de expressão, e da comunicação, a sociedade vivencia da última década até os dias atuais uma expansão enorme, viabilizada pelas inúmeras ferramentas de internet e pelas redes sociais. Dessa forma, a internet estreitou e aproximou as relações entre as pessoas e a forma como elas interagem umas com as outras.[32]

A liberdade de expressão então nesse campo das relações virtuais, se impõe como um princípio absoluto e até mesmo essencial para o estabelecimento dessa rede tecnológica de comunicação entre os indivíduos.

Mas, embora a sua importância seja inquestionável, há limites para a liberdade de expressão, nas comunicações virtuais? Essa garantia constitucional como direito fundamental, se sobrepõe a outros direitos fundamentais como o direito

[31]HIRATA, Alessandro. Direito à privacidade. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade> Acesso em 24 de set, 2021, 21:58.

[32] HIRATA, Alessandro. Direito à privacidade. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade> Acesso em 24 de set, 2021, 21:58.

à privacidade, direitos de personalidade, ou possui a mesma relevância de coexistência com os outros direitos?

O que tem sido demonstrado nesses tempos "modernos" em termos de comunicação, é que a liberdade de expressão mesmo como garantia fundamental não representaria um direito absoluto, e em diversos momentos entra em choque com outras garantias que resguardam a tutela jurisdicional. E nesses casos, parece ser democrático e ponderado, que o princípio da proporcionalidade, no sentido do peso e importância de cada garantia tutelada, permeie a análise do caso concreto na busca da solução do referido conflito.[33]

A própria Constituição Federal de 1988, proíbe de maneira taxativa o anonimato, determinando a exigência da identificação do autor das manifestações. Isso reflete um modelo de liberdade de expressão com responsabilidade, estabelecendo que os indivíduos que se expressarem de forma a desrespeitar direitos fundamentais dos outros, poderá ser responsabilizado e isso não reflete uma mitigação da liberdade de expressão e sim um cuidado para que esse direito não se sobreponha de maneira absoluta a outras garantias fundamentais, igualmente relevantes juridicamente e socialmente falando.[34]

A liberdade de expressão é um direito de extrema relevância e abrangência e com diversas implicações políticas, artísticas, ideologias individuais, atuação da imprensa, investigações, e uma infinidade de temas.

Assim, todo indivíduo tem a liberdade de expressão garantida e não há no Brasil legalmente instituída, uma censura prévia ao que cada um pretende publicar, mas a própria Constituição Brasileira em seu texto, ao dispor sobre outros direitos e garantias fundamentais, acaba por oferecer àqueles que se sentiram desrespeitados e

[33]HIRATA, Alessandro. Direito à privacidade. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade> Acesso em 24 de set, 2021, 21:58.

[34]HIRATA, Alessandro. Direito à privacidade. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade> Acesso em 24 de set, 2021, 21:58.

ofendidos, ferramentas para buscarem a responsabilização daqueles que ultrapassaram o "limite" da liberdade de expressão, submetendo garantias fundamentais de outros.[35]

A liberdade em geral, reflete um direito amplo, o que consiste em "ter" ou "não ter" tal garantia. O indivíduo é livre ou não. E os excessos porventura cometidos, encontram no ordenamento jurídico respaldo para que possam eventualmente ser responsabilizados. Assim, pode-se afirmar que a pessoa exerceu o seu direito à liberdade de expressão, e nesse exercício, ao desrespeitar os direitos de outras pessoas, poderá ter que responder por isso.[36]

Existe uma fronteira entre um direito e outro, e isso remete a uma expressão bastante conhecida: "o meu direito termina quando começa o do outro". Essa expressão não é muito clara, mas na prática e no tema dissertado no presente artigo, significa que, por exemplo, pode-se usar a liberdade de expressão para externar o que se acha sobre determinada pessoa, mas se essa manifestação desrespeitar direitos fundamentais dessa pessoa, quem se manifestou, exercendo o direito de liberdade de expressão, poderá ser responsabilizado cível ou penalmente.

O Marco Civil da Internet seguindo o mesmo raciocínio, e em estrita observância à Constituição Federal de 1988, dispõe que:

> "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."[37]

Dessa forma, o dever de reparação do dano em consequência do abuso da liberdade de expressão praticado na Internet e outros meios de comunicação é do usuário internauta e não do provedor de internet. Afinal, caso os provedores

[35] https://www.migalhas.com.br/coluna/constituicao-na-escola/287487/liberdade-de-expressao-em-tempos-de-internet

[36] BOTTI, Flávia. Principais aspectos jurídicos da liberdade de expressão. 2021. Disponível em < https://www.aurum.com.br/blog/liberdade-de-expressao/> Acesso em 29 de set, 2021, 16:35.

[37] BRASIL, Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 27 de set, 2021, 22:15.

tivessem essa responsabilidade, tal prática poderia ser configurada como uma espécie de censura e controle prévio, contrariando os princípios da intimidade e privacidade dos usuários, garantidos constitucionalmente.[38]

A referida lei estabelece que os provedores e internet somente poderão ser responsabilizados por danos causados por terceiros, caso após ordem judicial específica, não adote as diligências no sentido da indisponibilização do conteúdo, obedecendo aos prazos e limites técnicos dos seus serviços, ressalvadas claro, as disposições legais em contrário previstas no art 18 do Marco Civil da Internet.[39]

Ainda, nesse sentido, e com o objetivo de evitar a propagação e divulgação de violações a direitos dos indivíduos, e ainda de identificar o autor da manifestação, tendo em vista que a CF de 1988 veda o anonimato, a lei do Marco Civil determina aos provedores de aplicação de internet e conexão, a responsabilidade de guardar os registros pelo prazo de seis meses a um ano, dependendo do tipo de atividade dentro do processo. Assim, eventualmente esses registros poderão fazer a identificação individual do internauta, para que a responsabilização recaia somente sobre quem efetivamente causou o dano a outro.[40]

5 CONSIDERAÇÕES FINAIS

A liberdade de expressão consiste no direito que o indivíduo tem a se manifestar sobre as suas opiniões, conceitos e ideias, de acordo com os seus valores e vontades. Consiste no grande pilar das sociedades democráticas.

A liberdade de expressão é antes e tudo uma espécie de direito natural do ser humano. Isso porque o indivíduo nasce com uma condição humana, originária, de liberdade.

---

[38] DOMINGUES, Diego. Liberdade de expressão e novos meios de comunicação: limites, deveres e responsabilidades. 2016. Disponível em <https://diegosigoli.jusbrasil.com.br/artigos/345585288/liberdade-de-expressao-e-novos-meios-de-comunicacao-limites-deveres-e-responsabilidades >Acesso em 30 de set, 2021, 22:50.

[39] DOMINGUES, Diego. Liberdade de expressão e novos meios de comunicação: limites, deveres e responsabilidades. 2016. Disponível em <https://diegosigoli.jusbrasil.com.br/artigos/345585288/liberdade-de-expressao-e-novos-meios-de-comunicacao-limites-deveres-e-responsabilidades >Acesso em 30 de set, 2021, 22:50.

[40] DOMINGUES, Diego. Liberdade de expressão e novos meios de comunicação: limites, deveres e responsabilidades. 2016. Disponível em <https://diegosigoli.jusbrasil.com.br/artigos/345585288/liberdade-de-expressao-e-novos-meios-de-comunicacao-limites-deveres-e-responsabilidades >Acesso em 30 de set, 2021, 22:50.

A liberdade é um direito de conceito bastante amplo e não comporta mitigações no sentido de ser parcial. Entretanto, no caso da liberdade de expressão, apesar da dimensão, não se pode afirmar que esse direito é absoluto e se sobrepõe a quaisquer outros direitos protegidos pelo ordenamento jurídico.

Essa questão tem se tornado comum com a ascensão meteórica que o Brasil e o mundo vêm experimentando de uma década até a presente data, no desenvolvimento e expansão dos meios de comunicação virtuais com a utilização da Internet.

Com essa nova realidade, em 2014 foi sancionada a Lei 12.965, o Marco Civil da Internet, elaborado para determinar garantias, princípios e regras no ambiente da internet, garantindo assim, os direitos dos agentes envolvidos.

Um dos pilares do Marco Civil é a liberdade de expressão e com a utilização cada vez mais frequente da comunicação por meios virtuais, os indivíduos se manifestam cada vez mais sobre política, religião, futebol, disseminam suas ideias, formam opiniões, influenciam as pessoas.

E com essa propagação sem precedentes de opiniões e vozes, chega-se ao questionamento acerca da existência de imitações à liberdade de expressão, afinal, se eu posso me expressar da forma como penso e entendo, eu poderia também em nome do exercício desse direito, desrespeitar os direitos dos outros? O indivíduo em nome da liberdade de expressão poderia ofender a honra, a dignidade de alguém?

A CF de 1988 quando veda o anonimato de quem se manifesta e tutela vários outros direitos como a dignidade, privacidade, honra, intimidade, privacidade, significa que a liberdade de expressão é um direito tutelado e garantido, mas ele coexiste com outros direitos que precisam ser respeitados.

Não há no ordenamento jurídico brasileiro mitigação ou censura prévia à liberdade de expressão, mas caso no exercício da sua liberdade, o indivíduo desrespeite algum direito de outra pessoa, ele responderá por isso, pelo fato de cometido excesso com a sua liberdade de expressão. Afinal o ser humano está inserido em um contexto social, somos vários e todos gozamos da tutela jurídica do estado.

Então o exercício da liberdade de expressão poderá em muitos casos entrar em conflito com outros direitos fundamentais e bens jurídicos protegidos pelo estado. [41]

O direito à liberdade de expressão, por exemplo, não pode desrespeitar a dignidade humana. O Art. 5º da CF/88 trata da livre manifestação de pensamento, vedando o anonimato e garantindo a livre expressão de liberdade artística, intelectual, científica, de comunicação, que não dependem de censura ou licença para tal, ou seja, as pessoas podem se manifestar com total liberdade, mas isso não significa que em caso de desrespeito aos direitos dos outros, o indivíduo que assim o fez, não possa ser responsabilizado. Como exemplo, discursos de ódio contra minorias, violência contra mulheres, negros, que incentivam o terrorismo. Esses discursos são externados, sem censura prévia, mas implicarão em consequências para quem os desferiu, pelo fato dos danos causados a outras pessoas.[42]

Assim, a legislação específica que regulamenta essas relações no ambiente da rede de internet, apesar de possuir muitas lacunas, devido à velocidade de propagação das comunicações virtuais e do avanço da tecnologia, é considerado um avanço no sentido da tutela dos direitos a serem garantidos.

O Direito é uma ciência que nasce na sociedade, nas relações entre as pessoas, e é por meio da observação disso, que as leis são elaboradas., ajustando, preenchendo as lacunas legais e da tutela do Estado.

E paralelo a isso, os usuários precisam compreender que assim como o Direito tutela a segurança e os direitos das pessoas em casa, no trabalho, nas relações familiares, nas relações de consumo, nas atividades e em todos os ramos de atividades e relações sociais, no ambiente da internet não é diferente, e todos os

[41] HIRATA, Alessandro. Direito à privacidade. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade> Acesso em 24 de set, 2021, 21:58.

[42] MESQUITA, Gabriela. Quais os limites da liberdade de expressão na internet? 2019.Disponível em <https://www.brasildefato.com.br/2019/05/28/quais-os-limites-da-liberdade-de-expressao-na-internet > Acesso em 01 de out, 2021, 16:35.

direitos e garantias tutelados pelo ordenamento jurídico brasileiro têm a mesma validade dentro do espaço tecnológico.

Assim, a liberdade de expressão é um direito garantido pela constituição, é pilar da democracia, do Marco Civil da Internet, da construção de novas ideias e conceitos, mas não possui esse direito, o "direito" de desrespeitar outras garantias legais igualmente resguardadas. A sociedade democrática implica na coexistência de direitos e garantias que são prerrogativas de todos os indivíduos. Dessa forma, todos esses direitos deverão ser respeitados e garantidos, também nos ambientes virtuais.

REFERÊNCIAS

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil: texto constitucional promulgado em 5 de outubro de 1988, compilado até a Emenda Constitucional nº 109/2021. – Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2021. 426p.

HIRATA, Alessandro. Direito à privacidade. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade> Acesso em 24 de set, 2021, 21:58.

BRASIL, Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 27 de set. 2021.

BOTTI, Flávia. Principais aspectos jurídicos da liberdade de expressão. 2021. Disponível em < https://www.aurum.com.br/blog/liberdade-de-expressao/> Acesso em 29 de set. 2021.

BRASIL, Decreto 592 de 06 de julho de 1992. Dispõe sobre Atos internacionais. Pacto Internacional sobre direitos civis e políticos. Promulgação. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm > Acesso em 30 de set. 2021.

ALENCAR, Morgana. Tire suas dúvidas sobre o Marco Civil da Internet, 2021. Disponível em <https://www.aurum.com.br/blog/marco-civil-da-internet/ > Acesso em 30 de set. 2021.

RAMOS, Rahellen. O que é o Marco Civil da Internet? 06 de agosto de 2021. Disponível em:< https://www.politize.com.br/marco-civil-da-internet/ > Acesso em 29 de set. 2021.

FERREIRA, Fillipe. A proteção ao consumidor como direito fundamental constitucional: as garantias consumeristas. 01 de maio de 2018.Disponível em:<-https://ambitojuridico.com.br/edicoes/revista-172/a-protecao-ao-consumidor-como-direito-fundamental-constitucional-as-garantias-consumeristas/ > Acesso em 30 de set. 2021.

BRASIL. Lei 13.709, de 13 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >Acesso em 01 de out. 2021.

FIA, Fundação Instituto de Administração, 22 de setembro de 2020. Liberdade de expressão: lei, evolução, importância e limites. Disponível em <https://fia.com.br/blog/liberdade-de-expressao/> Acesso em 30 de set de 2021.

Disponível em: <https://www.migalhas.com.br/coluna/constituicao-na-escola/287487/liberdade-de-expressao-em-tempos-de-internet> Acesso em 29 de set, 2021.

AQUINO, Nick Richard. Antinomia jurídica entre o Marco Civil da Internet e o código de Defesa do Consumidor em matéria de Responsabilidade Civil dos provedores de aplicação de internet. Setembro de 2015. Disponível em:< https://jus.com.br/artigos/42861/antinomia-juridica-entre-o-marco-civil-da-internet-e-o-codigo-de-defesa-do-consumidor-em-materia-de-responsabilidade-civil-dos-provedores-de-aplicacoes-de-internet> Acesso em 30 de set. 2021.

DOMINGUES, Diego. Liberdade de expressão e novos meios de comunicação: limites, deveres e responsabilidades. 2016. Disponível em <https://diegosigoli.jusbrasil.com.br/artigos/345585288/liberdade-de-expressao-e-novos-meios-de-comunicacao-limites-deveres-e-responsabilidades >Acesso em 30 de set. 2021.

MESQUITA, Gabriela. Quais os limites da liberdade de expressão na internet? 2019.Disponível em <https://www.brasildefato.com.br/2019/05/28/quais-os-limites-da-liberdade-de-expressao-na-internet > Acesso em 01 de out. 2021.

ATAQUES CIBERNÉTICOS: A INSUFICIÊNCIA DA LEGISLAÇÃO BRASILEIRA E A POSSIBILIDADE DA RESPONSABILIZAÇÃO CIVIL DOS PROVEDORES POR INCIDENTE DE VAZAMENTO DE DADOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

Isabelly Alves de Melo[1]

RESUMO

O século XXI com o rápido avanço da tecnologia passou a ser chamado de Sociedade da Informação ou Era da Informação, estando inserida na quarta revolução industrial[2], onde informações e dados pessoais e/ou sensíveis se tornaram principais recursos econômicos das empresas, logo o principal alvo dos ataques cibernéticos. No Brasil existem poucas leis que abordam sobre os crimes virtuais, consequentemente os infratores ficam livres de punição. Por esse motivo, o legislador através da promulgação da Lei Geral de Proteção de Dados, objetivou a proteção de dados pessoais e/ou sensíveis, contemplando um regramento de responsabilização em caso de violações possíveis vazamentos. Contudo, questiona-se sobre a suficiência da legislação brasileira para os crimes cibernéticos e em casos de vazamento de dados quem se responsabilizaria civilmente? Assim, através de um viés metodológico dedutivo, o presente artigo irá estudar e analisar a suficiência da legislação brasileira para os crimes cibernéticos em contraposição com a responsabilização civil dos provedores pelo vazamento de dados, principalmente nos casos de ataques cibernéticos previsto na Lei Geral de Proteção de Dados.

Palavras-chave: Responsabilidade Civil. Ataques Cibernéticos. Lei Geral de Proteção de Dados. Ordenamento Brasileiro.

[1] Graduada em Direito pelo Centro Universitário de Brasília - UniCEUB. Advogada. Aluna de Pós-Graduação Lato Sensu em Direito Público do Centro Universitário de Brasília – UniCEUB/ICPD. E-mail: belly.alves967@gmail.com

[2] BARBOSA, Marcos T. J.; BAISSO, Marcos; ALMEIDA, Marcos T. Surge uma nova sociedade. In: SILVA, Elcio B.; SCOTON, Maria L. R. P. D.; PEREIRA, Sérgio L.; DIAS, Eduardo M. Automação & sociedade: Quarta Revolução Industrial, um olhar para o Brasil. São Paulo: Brasport, 2018.

ABSTRACT

The 21st century with the rapid advancement of technology has come to be called the Information Society or Information Age, being inserted in the fourth industrial revolution, where personal and/or sensitive information and data have become the main economic resources of companies, thus the main target of cyber attacks. In Brazil there are few laws that address virtual crimes, consequently the offenders are free from punishment. For this reason, the legislator, through the enactment of the General Law of Data Protection, aimed at protecting personal and/or sensitive data, contemplating a regulation of accountability in case of possible violations or leaks. However, the question arises as to the sufficiency of the Brazilian legislation for cybercrime and, in cases of data leakage, who would be held civilly liable? Thus, through a deductive methodological approach, this article will study and analyze the sufficiency of the Brazilian legislation for cybercrime in opposition to the civil liability of providers for data leakage, especially in cases of cyberattacks provided in the General Law of Data Protection.

Keywords: Civil Liability. Cyber Attacks. General Law of Data Protection. Brazilian Law.

1 INTRODUÇÃO

Com o acelerado avanço tecnológico a sociedade do Século XXI passou a ser chamada como sociedade da informação ou era da informação, estando enquadrada na quarta revolução industrial[3]. Esta abrangência da evolução tecnológica trouxe consigo diversos benefícios, entretanto com eles vieram diversas categorias de crimes e criminosos que utilizam as mais variadas estratégias para atuar nesta área da tecnologia, conhecidos como crimes cibernéticos ou crimes virtuais. Com esta problemática, os cidadãos estão receosos com a impunidade que esses crimes ficam no Brasil, tudo isso devido à falta de uma legislação específica.

Apenas em 2012 o legislador procurou criar leis que abordem os crimes praticados no meio virtual, principalmente a tipificação do crime de invasão tecnológica. Entretanto, diversas condutas danosas não foram tipificadas pela lei, como, por exemplo, os vírus utilizados para danificar o sistema de computadores, a destruição de dados, entre outros. Apesar das diversas falhas apresentada pela Lei Carolina Dieckmann, o legislador apenas em 2014 através do Marco Civil da

[3] BARBOSA, Marcos T. J.; BAISSO, Marcos; ALMEIDA, Marcos T. **Surge uma nova sociedade**. In: SILVA, Elcio B.; SCOTON, Maria L. R. P. D.; PEREIRA, Sérgio L.; DIAS, Eduardo M. **Automação & sociedade: Quarta Revolução Industrial, um olhar para o Brasil**. São Paulo: Brasport, 2018.

Internet trouxe uma lei com conceitos e fundamentos informáticos, porém ainda vazio ao que se trata da tipificação e punição dos crimes praticados neste meio.

Assim, o surgimento da Lei Carolina Dieckmann e Marco Civil da Internet possibilitaram avanços no combate aos crimes virtuais, entretanto, a legislação é insuficiente para combater a criminalidade virtual, haja vista ser um campo em constante evolução, deixando os criminosos impunes ou com uma pena branda se comparado com a gravidade do crime praticado. Em contrapartida, a promulgação da LGPD demonstra a importância da proteção dos dados pessoais e/ou sensíveis e determina a regulação da proteção destes dados suprindo as eventuais lacunas legislativas existentes nas leis atuais.

De modo a assegurar a proteção de dados pessoais, apesar dos criminosos saírem impune dos crimes cometidos, o legislador estabeleceu regras para a reparação de dano patrimonial e moral ocasionado por agentes de tratamento, responsabilizando, portanto, controladores de dados de forma objetiva, principalmente nos casos de ataques cibernéticos, um dos principais crimes praticados no meio virtual que aumentou exponencialmente na pandemia do (Covid-19).

Contudo, a Lei Geral de Proteção de dados não abarca os crimes virtuais praticados, necessitando de uma lei complementar que tipifica e pune os crimes praticados no meio virtual. Assim, demonstra a relevância deste estudo que se encontra na insegurança que a sociedade atual experimenta, visto que a tecnologia evolui com as práticas delituosas no meio virtual e já a legislação encontra-se estagnada.

A partir disto, através do método dedutivo, o presente artigo pretende examinar a problemática da insuficiência das leis atualmente existentes no Brasil para a punição dos agentes que cometem os crimes cibernéticos. Em contrapartida, o artigo demonstra a punição prevista na Lei Geral de Proteção de dados em casos de vazamentos de dados pessoais e/ou sensíveis cometidos através dos ataques cibernéticos.

2 CRIMES CIBERNÉTICOS

Atualmente estamos vivendo na Era da Informação, onde o acesso e o compartilhamento de informações se tornaram algo essencial e cotidiano na vida das pessoas. A sociedade está diariamente conectada à internet, seja para acesso a sistemas de interação como: e-mails, videoconferências, Instagram ou para operações bancárias, sendo estes recursos vantajosos, principalmente quando o mundo teve que passar por uma pandemia, onde o contato era algo inviável.

Como nem tudo são vantagens, através da conexão de milhares de pessoas com altas capacidades técnicas ou sem aprendem diversas formas de como praticar o ilícito, principalmente através da criação de um dispositivo conhecido como Malware, aplicativo este "que adentra um sistema, com intenção de repassar informações a outrem ou causar danos ao sistema operacional de dispositivos eletrônicos, dependendo da interação da pessoa"[4]. Além deste, existe também os Worms que independe de interação humana que se aproveita das "falhas do dispositivo e se hospeda no sistema"[5]. Assim, os malwares é o principal ativo de repasse de informações que originam os cibercrimes.

2.1 Evolução histórica: surgimento da internet e dos crimes virtuais

O meio virtual sofreu inúmeras ampliações após a evolução tecnológica, facilitando "a globalização econômica social e cultural"[6], fazendo com que a distância física fosse encurtada, proporcionando relacionamentos e a comunicação entre os familiares através de dispositivos tecnológicos, passando a fazer parte da rotina das pessoas, das empresas e do governo.

Contudo, com os benefícios da facilidade de acesso à informação surgiram novas formas de violação dos bens jurídicos protegidos pela Carta Magna, transcendendo o plano físico para o plano virtual cometendo os chamados crimes

[4] DIEGO, Cruz; RODRIGUES, Juliana. **Crimes Cibernéticos e a falsa sensação de impunidade.** Revista Cientifica Eletrônica do Curso de Direito, 13º ed., janeiro de 2018.
[5] DIEGO, Cruz; RODRIGUES, Juliana. **Crimes Cibernéticos e a falsa sensação de impunidade.** Revista Cientifica Eletrônica do Curso de Direito, 13º Edição, Janeiro de 2018.
[6] VIDAL, Rodrigo de Mello. **Crimes Virtuais.** 2015. 13f. Tese (Pós-graduação em Direito Público) – Universidade Candido Mendes, Rio de Janeiro, 2015;

virtuais ou crimes cibernéticos, onde o desconhecimento de outros tornaram-se o poder e lucro para alguns.

Os crimes virtuais ou crimes cibernéticos são cometidos no chamado ciberespaço, um mundo "de comunicação em que não é necessária a presença física do homem para constituir a comunicação, a interconectividade e o espaço que interligam pessoas, documentos e máquinas"[7] principalmente através da internet.

Os crimes cibernéticos ou os cibercrimes são conhecidos por serem uma atividade criminosa que utiliza o computador ou uma rede de computadores conectados a uma rede para realizar o crime, com intuito de adquirir dinheiro através do roubo de dados pessoais e/ou sensíveis de pessoas ou organizações. Portanto, os crimes cibernéticos "são como os crimes comuns, tendo condutas típicas, antijurídicas e culpáveis, porém sendo praticadas com a utilização da informática"[8].

Feliciano define o crime cibernético como:

> "Recente fenômeno histórico-sociocultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que tem por objeto material ou meio de execução o objeto tecnológico informático" (2000, p.13)

Com a universalização da internet e o aumento de compartilhamento das informações, os dados pessoais e/ou sensíveis se tornaram o principal ativo do mercado eletrônico e devido à pandemia do (Covid-19) houve uma migração do sistema para a internet de forma exponencial aumentando os crimes cibernéticos em proporções nunca vista.

Diante deste aumento de crimes cibernéticos um dos principais problemas avistados é a dificuldade de identificar o Autor da prática do ato lesivo, ou seja, determinar o autor do crime. O mundo virtual por si só facilita o anonimato de seus usuários ou disponibiliza recursos ao indivíduo para se passar por outra pessoa, através de dados pessoais e/ou sensíveis roubados, tornando ainda mais complexo a identificação do autor do crime dificultando ainda mais a descoberta do autor.

---

[7] SANTOS, Liara Ruff dos Santos; MARTINS, Luana Bertasso; TYBUSCH, Francielle Benini Agne. **Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo.** Santa Maria, Edição 2017. Congresso Internacional de Direito e Contemporaneidade.

[8] MELO, Mateus Ramos. **Direito digital: crimes cibernéticos e marco civil da Internet.**

Assim, diante das novas relações sociais e do avanço do compartilhamento das informações e dados pessoais e/ou sensíveis no mercado eletrônico, torna-se razão suficiente para que a legislação brasileira se adapte a esta nova era, conhecida como Era da Informação, visando combater essas infrações penais cometidas no ambiente virtual.

2.2 Aplicação da legislação brasileira nos crimes cibernéticos

A Constituição Federal em seu art. 5º, inciso XXXIX determina que "*não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal"*, isto é, para tornar possível a punição desses crimes praticados no meio virtual. O tipo penal deve-se adequar nas normas existentes e caso as lacunas persistam devem ser preenchidas com outra lei. Lembrando que as novas leis que surgirem devem incorporar os conceitos de informática.

No Brasil, antes da promulgação da Lei nº 17.735/12 e a Lei nº 12.737/12, conhecido como a Lei Carolina Dieckmann, não havia leis direcionadas para os crimes cometidos no meio virtual, abordando apenas os crimes de forma geral sem especificar o meio utilizado para a sua prática. Contudo, após o ocorrido com a atriz foi evidenciado a necessidade de uma lei específica para os crimes cometidos no meio virtual.

Assim, a Lei nº 12.737/12 passou a tipificar um dos crimes cometidos no ambiente virtual, trazendo alterações no Código Penal, onde foi acrescido os artigos 154-A e 154-B, o qual aborda sobre a invasão de dispositivo informático. Além disso, alterou os artigos 266 e 298 do Código Penal. Com esse avanço, o Brasil passou a sujeitar os autores deste crime de invasão de dispositivo com uma pena de três meses a um ano de prisão e multa.

Apesar da promulgação da Lei Carolina Dieckmann, surgiram diversas críticas referente ao crime criado, principalmente quanto ao sujeito ativo, pois a Lei delimitou quem pudesse praticar o crime quando, na verdade, qualquer um que cometesse o crime deveria ser punido "não devendo importar quem quer que o

praticou”[9]. Outra falha encontrada pelos doutrinadores refere-se aos mecanismos de segurança, uma vez usuário da internet inexperiente, isto é, não recorre a aparatos de segurança, não será amparado pelos artigos, sendo, portanto, considerado “o crime atípico”[10]. Carneiro (2012), diz:

> É evidente que a lei restringe a tipicidade da invasão aos casos em que há violação indevida de mecanismo de segurança, sendo assim, os dispositivos informáticos não dotados de ferramentas de proteção estariam excluídos da aplicação legal. Mas em se tratando de expressões como mecanismos de segurança e dispositivos informáticos como, por exemplo: hardwares e softwares não foram definidos na lei, restando dúvidas sobre o completo enquadramento de certos casos.

Como se não bastassem as falhas ora citadas, a pena apresentada pela lei para um crime com conduta de médio potencial ofensivo, pode ser cumprida em regime semiaberto ou imediatamente aberto, isto é, uma conduta que pode causar danos irreversíveis a suas vítimas, tem uma punição branda e pouco impactante, não tendo o principal objetivo das leis que é desmotivar a sua prática.

Ante as lacunas existentes quanto aos crimes virtuais em 2014 foi promulgada a Lei nº 12.965, intitulada como “Marco Civil da Internet” trazendo em seu corpo, fundamentos, conceitos e direitos dos usufruidores. Além disso, tipifica princípios, garantias, direitos e deveres no ambiente virtual. Contudo, é evidente que a punição ao desrespeito de tais princípios é branda não atingindo um resultado satisfatório. Como se não bastasse, atualmente, as requisições de informações privadas necessitam de uma ordem judicial, não podendo o provedor da internet fornecer dados como IP, senha e logins utilizados pelos criminosos, tornando o trabalho de investigação moroso.

Assim é evidente que apesar da tipificação de garantias, princípios, direitos e deveres as leis atualmente existentes não abarcam por completo o campo de atividades dos criminosos virtuais, isto é, os crimes cibernéticos em espécie, pois o legislador tem se preocupado com o momento e não a longo prazo, ocasionando

[9] SANCHES, Ademir Gasques. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em: https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil. Acesso em: 17 set. 2021;

[10] ANCHES, Ademir Gasques. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em: https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil. Acesso em: 17 set. 2021;

diversas lacunas que ficam à mercê de outras legislações que julgam com base no efeito danoso causado pelos infratores.

Com isso, a real problemática dos crimes cibernéticos encontra-se na falha de uma lei que classifica, pune e demonstra as "questões técnicas de como chegar no infrator e de quem é a competência para julgar"[11]. É indiscutível que o ordenamento jurídico brasileiro não está conseguindo acompanhar os avanços dos crimes virtuais, tornando-se um "grande entrave para desenvolver soluções definitivas para o problema da má utilização da rede mundial de computadores"[12].

Assim, enquanto o legislador encontra-se perdido no meio de tanto avanço tecnológico cumulado com o surgimento de diversos crimes cibernéticos, incluindo os ataques cibernéticos às empresas privadas e públicas aumentados exponencialmente durante a pandemia do (Covid-19), a promulgação da LGPD veio para enfatizar e estabelecer a proteção de dados pessoais como algo essencial na vida do cidadão, punindo, inclusive os agentes de tratamento de dados pessoais e/ou sensíveis nos casos de vazamento destes dados, ou seja, enquanto retroagimos em relação à tipificação e punição penal dos crimes virtuais praticados, a Lei Geral de Proteção de dados pune os provedores que não adotarem as medidas de segurança previstas em seu corpo, demonstrando a necessidade e a urgência de uma lei que traga os conceitos de informáticas para o ordenamento brasileiro para que assim os autores dos crimes virtuais sejam devidamente punidos.

3 A RESPONSABILIDADE CIVIL NA LGPD

Como dito anteriormente, apesar da promulgação da Lei Geral de Proteção de Dados, o ordenamento jurídico brasileiro se encontra defasado em uma lei que aborde os conceitos e fundamentos da informática para tipificar e punir os crimes virtuais cometidos. Entretanto, em meio ao avanço tecnológico a LGPD demonstrou a necessidade da proteção dos dados pessoais e/ou sensíveis, haja vista a crescente utilização dos meios digitais e consequentemente a prática dos crimes cibernéticos.

[11] CRUZ, Diego; RODRIGUES, Juliana. **Crimes Cibernéticos e a falsa sensação de impunidade.** Revista Científica Eletrônica do Curso de Direito, janeiro de 2012, 13ª Edição.
[12] CAZAROTI, Tatiane Martins Barros. **Crimes Cibernéticos.** Artigo Científico.

A Lei Geral de Proteção de dados regulamenta no Brasil a transferência e a proteção de dados pessoais e/ou sensíveis, seja em âmbito privado ou no âmbito público, determinando para tanto quem são seus agentes envolvidos e a responsabilidade civil por incidentes. Assim, a lei impacta as empresas do ramo diretamente, podendo determinar multa por não cumprir as medidas de segurança e os princípios previstos.

A par deste novo cenário, onde os dados são o principal ativo do mercado e a falta de uma legislação específica que abordasse a proteção destes dados, em 2020 entrou em vigor a Lei n.º 13.709/2018 – Lei Geral de Proteção de Dados, objetivando resgatar e demonstrar a necessidade da proteção dos dados pessoais e/ou sensíveis. Assim, existindo danos, advindos da manipulação de dados e falta de segurança, a reparação civil se mostra a medida mais adequada a vítima, tendo em vista que atualmente não há punição devida ao Autor do crime cibernético.

Dessa forma, visando proteger o titular dos dados pessoais e/ou sensíveis, a LGPD, na Seção III do Capítulo VI intitulado "Da Responsabilidade e do Ressarcimento de Danos", instituiu regras para a reparação de dano patrimonial e moral praticado pelos agentes de tratamento de dados com base nos princípios da finalidade, da qualidade dos dados, da adequação, da necessidade etc. e nos demais atos normativos que versem sobre a proteção de dados pessoais.

Antes de avançarmos, convém conceituar dados pessoais e sensíveis previsto no inciso I do artigo 5º da Lei ora citada, como sendo aqueles dados relacionados a pessoa natural permitindo a sua identificação ou que tornam a pessoa identificável[13].

Além disso, a Lei estabelece no inciso X do artigo 5º um rol exemplificativo das atividades de tratamento de dados pessoais pelos seus agentes controlador e operador, consistindo em "toda operação realizada com dados pessoais[14] ", tais como: coleta, classificação, produção, processamento utilização, arquivamento e armazenamento de dados.

[13] BIONI, Bruno Ricardo**. Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. p. 61;

[14] COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 3. ed. rev., atual e ampl. São Paulo: 2019. p. 75;

Superados tais conceitos, a legislação atual preceitua que a desobediência a um dever jurídico configura ato ilícito, logo gera o dever de reparar o dano causado a outrem. Neste contexto, é possível identificar na LGPD em seus artigos 42, caput, artigo 44, parágrafo único e artigo 46, duas situações de responsabilidade civil: (i) "violação das normas jurídicas, do microssistema de proteção de dados e (ii) violação de normas técnicas, voltadas à segurança e proteção de dados pessoais"[15], devendo estar presente três elementos primordiais para a responsabilização do agente, sendo a: (i) nexo de causalidade; (ii) ação ou omissão; (iii) dano.

Assim como a reparação de dano previsto no Código Civil a LGPD estabelece excludentes da responsabilidade dos agentes de tratamento quando: "(i) que não realizaram o tratamento de dados pessoais que lhes é atribuído; (ii) que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou (iii) que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros"[16].

3.1 Responsabilização dos provedores por vazamento de dados em ataques cibernéticos

A Lei Geral de Proteção de Dados distingue o controlador em ente público e em pessoa natural ou pessoa jurídica de direito privado. Entretanto, antes de avançarmos na responsabilização civil nos casos de ataques cibernético, importante ressaltar que o Brasil é o quarto maior país em casos de ciber ameaças e de ransoware, vírus do "tipo 'malware'. Para melhor esclarecimento:

> Os *ransomware* são, já há um tempo, uma das ameaças mais comuns a sistemas públicos e privados no mundo inteiro. A obtenção desse tipo de *malware* por criminosos exige apenas que eles saibam onde procurar na Internet. A invasão só precisa encontrar uma vulnerabilidade: um sistema operacional ou aplicativo desatualizado, uma falha na configuração de um servidor ou até o despreparo de um usuário com poder de acesso ao sistema, que pode ter suas credenciais obtidas pelo criminoso, por exemplo, através de *link* em um endereço eletrônico fraudulento. A

[15] CAPANEMA, Walter Aranha. **A responsabilidade Civil na Lei Geral de Proteção de Dados.** Cadernos Jurídicos, São Paulo, ano 21, nº53, p.163-170, janeiro-março/2020;

[16] BRASIL. Lei nº 13/709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 10 abr. 2021;

> comunicação entre o criminoso e a vítima, assim como o pagamento do resgate, se dão por meios que dificultam o rastreamento e o trabalho da polícia. Juntas, essas características tornam os custos para o invasor baixíssimo se comparados aos potenciais retornos financeiros.[17]

Diante disso, com a promulgação da lei as empresas privadas e os entes públicos se viram obrigados a revisar seus procedimentos adotados tendo que "editar novas políticas de privacidade, termos de consentimento e planos de contingenciamento vocacionados à proteção de dados visando a assegurar a real privacidade e segurança das informações"[18].

Quando o controlador é um ente público a referida Lei citou em seu capítulo IV "Do tratamento de dados pessoais pelo Poder Público" os deveres da administração pública e traçou normas reguladoras do uso compartilhado do banco de dados entre os órgãos da administração pública. E por fim, proclamou o dever da observância da responsabilização e prestação de conta e de a submissão aos princípios da segurança e da prevenção.

A responsabilidade civil dos entes públicos no espectro das atividades de tratamento de dados pessoais se baseia no fundamento da teoria do risco administrativo, isto é, "se caracteriza na possibilidade de exposição e utilização indevida ou abusiva dos dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste"[19]. Além disso, a responsabilidade civil destes controladores tem como parâmetro os critérios da responsabilidade objetiva para os atos comissivos e subjetiva para os atos omissivo.

---

[17] SALVADOR, João Pedro Favaretto; GUIMARÃES, Tatiane. **O ataque ao STJ é mais um grito de socorro da segurança cibernética do Brasil.** FGV Artigos: 2020. Disponível em: https://portal.fgv.br/artigos/ataque-ao-stj-e-mais-grito-socorro-seguranca-cibernetica-brasil. Acesso em: 10 abr. 2021;

[18] FIGUEIREDO, Elisa Junqueira; FIATKOSKI, Nahyana Viott. **O que os recentes ataques cibernéticos nos ensinam sobre a LGPD.** Migalhas: 2020. Disponível em: https://www.migalhas.com.br/depeso/336280/o-que-os-recentes-ataques-ciberneticos-nos-ensinam-sobre-lgpd. Acesso em: 10 abr. 2021.

[19] PEREIRA, Flávio Henrique Unes; ALVIM, Rafael da Silva. **O regime da responsabilidade do Estado na Lei Geral de Proteção de Dados.** Conjur: 2020. Disponível em: https://www.conjur.com.br/2020-nov-22/pereira-alvim-regime-responsabilidade-estado-lgpd. Acesso em: 10 abr. 2021;

Nesta última hipótese, entende-se que caso ocorra o vazamento de dados pessoais por ente público através de uma brecha no banco de dados ensejará o dever de indenizar, principalmente por dano moral.

Já o controlador pessoa natural ou pessoa jurídica de direito privado quando se trata de incidente que gera danos aos consumidores, a possibilidade de responsabilização objetiva, isto é, que independe de culpa, aplicando o que preceitua o nosso Código de Defesa do Consumidor.

A regra é a aplicação da responsabilidade objetiva nos casos comprovados a falta de adoção das medidas de segurança estipuladas na LGPD por parte do controlador que realiza o tratamento de dados. Esta regra está amparada na rápida transição que a sociedade vem enfrentando para o mundo eletrônico, haja vista que esta velocidade pode fazer com que as plataformas criadas sejam desenvolvidas sem priorizar as medidas de segurança, criando um ambiente de vulnerabilidade.

Contudo, em situações em que os agentes de dados agirem conforme as normas de segurança, o caso deverá ser analisado à luz da responsabilidade subjetiva. Entretanto, importante deixar claro que "a mera invasão por terceiros não tem o condão de afastar por completo a responsabilidade do agente"[20], podendo caber nestes casos a responsabilidade de culpa concorrente, pois é impossível "afirmar de plano de que os agentes de tratamento de dados em nada contribuíram para a ocorrência do evento danoso"[21]

Diante disso, nos casos em que ocorra o vazamento de dados pessoais e/ou sensíveis através do cometimento de um crime virtual, como o ataque cibernético os agentes de tratamento de dados podem ser responsabilizados civilmente de forma objetiva. Este cenário não está muito distante dos brasileiros, basta darmos uma pesquisada e será possível visualizar diversos ataques cibernéticos ocorrido em um curto período como o ataque sofrido pelo STJ, pea Loja Renner, Facebook,

[20] MORAIS, Elisa Guimarães; SILVA, Janielle Magalhães. **Qual a resposta da LGPD para a responsabilização de agentes frente ao vazamento de dados por hackers?** Disponível em: https://www.migalhas.com.br/depeso/328337/qual-a-resposta-da-lgpd-para-a-responsabilizacao-de-agentes-frente-ao-vazamento-de-dados-por-hackers. Acesso em: 15 set. 2021;

[21] MORAIS, Elisa Guimarães; SILVA, Janielle Magalhães. **Qual a resposta da LGPD para a responsabilização de agentes frente ao vazamento de dados por hackers?** Disponível em: https://www.migalhas.com.br/depeso/328337/qual-a-resposta-da-lgpd-para-a-responsabilizacao-de-agentes-frente-ao-vazamento-de-dados-por-hackers. Acesso em: 15 set. 2021;

Netshoes, Uber, TSE, entre outros, estas organizações sofreram ataques e quase todas tiveram os dados de seus clientes/usuários vazados.

É evidente que a LGPD é rígida quando se trata de *tratamento de dados pessoais e/ou sensíveis* por intermédio de seus agentes, punindo-os quando não observarem as medidas de segurança, deixando os dados de seus titulares vulneráveis e à mercê de criminosos. Contudo, a LGPD não é suficiente para proteger os titulares destes ataques e possíveis vazamentos, necessitando de uma lei complementar na área criminalística que venha tipificar e punir os autores destes crimes virtuais, o que atualmente ainda não é possível vislumbrar, pois, as leis atualmente existentes são totalmente insuficientes ante as novas condutas para a prática de crimes.

Assim, a posição adotada pela LGPD ante os vazamentos de dados evidência ainda mais a necessidade de uma lei específica para punir o outro responsável, isto é, o autor do crime de vazamento e grita para o legislador a importância dos dados pessoais e/ou sensíveis demonstrando não ser necessário um evento grave para ele poder agir criando leis e regras que funcionem a longo prazo, punindo devidamente os praticantes dos crimes virtuais que visam lesar não só a vítima, mas o controlador.

4 CONCLUSÃO

A internet surgiu com o propósito de compartilhar a informação com toda a sociedade e aumentar as formas de comunicação entre as pessoas. A partir daí a internet se difundiu por todo o mundo se tornando um dos maiores veículos de comunicação mais utilizado nos últimos tempos. Com esta necessidade da digitalização em qualquer área surgiu também a necessidade de proteger os dados fornecidos através da rede de informática contra possíveis casos de vazamento/roubo de propriedade intelectual, uma das desvantagens da tecnologia que viola os direitos fundamentais.

Assim, algo criado para beneficiar os seus usuários e facilitar a vida do cidadão tornou-se uma ferramenta de ameaça ao longo dos anos, haja vista que atualmente os dados pessoais e/ou sensíveis se tornaram um dos principais ativos do

mercado eletrônico, virando, portanto, alvo dos crimes cometidos através de computadores conhecidos como crimes cibernéticos que geram lucros aos invasores.

Portanto, considerando o avanço tecnológico assimilado principalmente pelos criminosos, pôde se perceber através do presente trabalho que a atual legislação brasileira não está conseguindo atuar de forma positiva nesta evolução tecnológica, tendo em vista que não há leis específicas que abordem os crimes virtuais atualmente existentes. Assim, ficou claro que há a necessidade de elaboração de leis específicas e medidas a serem adotadas pelo Estado em relação aos crimes virtuais, haja vista que as Leis existentes são falhas e possuem lacunas no que diz respeito aos crimes cibernéticos.

De modo a evidenciar essa falha no Legislativo quanto a temática de crimes cibernéticos surge a Lei Geral de Proteção de dados mostrando a importância de se proteger os dados pessoais e/ou sensíveis coletados de seus usuários, estabelecendo regras, princípios e normas de segurança para os agentes de tratamento. Com isso, caso haja uma violação deste direito e ocasione danos ao seu titular caberá a responsabilização do agente de tratamento de forma objetiva independente se o vazamento ocorreu por um crime virtual, como os ataques cibernéticos.

Contudo, apesar de termos uma lei que responsabiliza os agentes de tratamento não há lei no ordenamento jurídico brasileiro que abarque e tipifique as novas condutas utilizadas para o cometimento de crimes no meio virtual, sendo assim, conforme o princípio da reserva legal, não possuem a possibilidade de serem punidas. Assim, deve o legislativo acordar e acompanhar o estado atual da nossa sociedade, aplicando inclusive a segurança cibernética que desempenha um papel importante no desenvolvimento da tecnologia da informação, tornando a internet mais segura.

REFERÊNCIAS

BARBOSA, Marcos T. J.; BAISSO, Marcos; ALMEIDA, Marcos T. Surge uma nova sociedade. In: SILVA, Elcio B.; SCOTON, Maria L. R. P. D.; PEREIRA, Sérgio L.; DIAS, Eduardo M. Automação & sociedade: Quarta Revolução Industrial, um olhar para o Brasil. São Paulo: Brasport, 2018;

BIONI, Bruno Ricardo**. Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. p. 61;

BRASIL. Lei nº 13/709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm Acesso em: 10 abr. 2021;

CAPANEMA, Walter Aranha. **A responsabilidade Civil na Lei Geral de Proteção de Dados.** Cadernos Jurídicos, São Paulo, ano 21, nº53, p.163-170, janeiro-março/2020;

CARNEIRO, Adeneele Garcia. **Crimes Virtuais: Elementos para uma reflexão sobre o problema na Tipificação.** Postado em 2012. Disponível em: http://www.egov.ufsc.br/portal/conteudo/crimes-virtuais-elementos-para-umareflex%C3%A3o-sobre-o-problema-na-tipifica%C3%A7%C3%A3o. Acesso em: 10 set. 2021;

CAZAROTI, Tatiane Martins Barros. **Crimes Cibernéticos.** Artigo Científico;

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 3. ed. rev., atual e ampl. São Paulo: 2019. p. 75;

DIEGO, Cruz; RODRIGUES, Juliana. **Crimes Cibernéticos e a falsa sensação de impunidade.** Revista Cientifica Eletrônica do Curso de Direito, 13ª Edição, janeiro de 2018;

FIGUEIREDO, Elisa Junqueira; FIATKOSKI, Nahyana Viott. **O que os recentes ataques cibernéticos nos ensinam sobre a LGPD.** Migalhas: 2020. Disponível em: https://www.migalhas.com.br/depeso/336280/o-que-os-recentes-ataques-ciberneticos-nos-ensinam-sobre-lgpd. Acesso em: 10 abr. 2021;

FELICIANO, Guilherme Guimarães. **Informática e criminalidade: parte I, Lineamentos e Definições.** Boletim do Instituto Pedro Pimentel, São Paulo, v. 13, n 2, 2000;

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lei Geral de Proteção de Dados Comentada**. 2. Ed. ver. Atual e Ampl. São Paulo: 2020, p.22;

MELO, Mateus Ramos. **Direito digital: crimes cibernéticos e marco civil da Internet.** Artigo Científico;

MORAIS, Elisa Guimarães; SILVA, Janielle Magalhães. **Qual a resposta da LGPD para a responsabilização de agentes frente ao vazamento de dados por hackers?** Disponível em: https://www.migalhas.com.br/depeso/328337/qual-a-resposta-da-lgpd-para-a-responsabilizacao-de-agentes-frente-ao-vazamento-de-dados-por-hackers. Acesso em: 15 set. 2021;

PEREIRA, Flávio Henrique Unes; ALVIM, Rafael da Silva. **O regime da responsabilidade do Estado na Lei Geral de Proteção de Dados.** Conjur: 2020. Disponível em: https://www.conjur.com.br/2020-nov-22/pereira-alvim-regime-responsabilidade-estado-lgpd. Acesso em: 10 abr. 2021;

SALVADOR, João Pedro Favaretto; GUIMARÃES, Tatiane. **O ataque ao STJ é mais um grito de socorro da segurança cibernética do Brasil.** FGV Artigos: 2020. Disponível em: https://portal.fgv.br/artigos/ataque-ao-stj-e-mais-grito-socorro-seguranca-cibernetica-brasil. Acesso em: 10 abr. 2021;

SANCHES, Ademir Gasques. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em: https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil. Acesso em: 17 set. 2021;

SANTOS, Liara Ruff dos Santos; MARTINS, Luana Bertasso; TYBUSCH, Francielle Benini Agne. **Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo.** Santa Maria, Edição 2017. Congresso Internacional de Direito e Contemporaneidade;

SCALETSCKY, Rodrigo Livtin; VAZ, Caroline. **A responsabilidade dos agentes de tratamento de dados pessoais no âmbito da Lei n.º 13.709/2018.** Disponível em: https://www.pucrs.br/direito/wp-content/uploads/sites/11/2021/01/rodrigo_scaletscky.pdf. Acesso em: 10 abr. 2021;

SCHWAB, Klaus. **Aplicando a Quarta Revolução Industrial**. São Paulo: Edipro, 2018;

VIDAL, Rodrigo de Mello. **Crimes Virtuais.** 2015. 13f. Tese (Pós-graduação em Direito Público) – Universidade Candido Mendes, Rio de Janeiro, 2015;

AS CRIPTOMOEDAS E A UTILIZAÇÃO DO SISTEMA FINANCEIRO PARA CONSTITUIÇÃO DE CRIMES DIGITAIS

Letícia de Amorim Pereira

RESUMO

O presente artigo tem o objetivo de demonstrar a utilização do sistema financeiro para a utilização das criptomoedas na configuração de crimes digitais. Com o avanço tecnológico, as formas de aplicação de recursos modificaram e se adaptaram a necessidade do mercado e dos consumidores. Assim, o incentivo à aplicação de recursos financeiros em diversificados tipos de investimentos culminou na popularização destas modalidades e consequentemente na abertura de mercado para diversas categorias de empresas. Em especial, entre elas, estão aquelas que operam moedas digitais. No entanto, este mercado, mostrou-se extremamente problemático o caminho ao crime digital tornou-se excessivamente estreito.

Palavras-chave: moeda digital; mercado financeiro; crime digital.

ABSTRACT

This article aims to demonstrate the use of the financial system for the use of cryptocurrencies in the configuration of digital crimes. With technological advances, the ways of applying resources have changed and adapted to the needs of the market and consumers. Thus, the incentive to invest financial resources in diversified types of investments culminated in the popularization of these modalities and, consequently, in the opening of the market for different categories of companies. In particular, among them are those that operate digital currencies. However, this market, proved to be extremely problematic, the path to cybercrime became excessively narrow.

Keywords: digital currency; financial market; digital crime

1 INTRODUÇÃO

As transformações vividas pelas organizações a partir dos avanços tecnológicos demonstraram a necessidade de atenção para específico nicho desta era. Qual seja, a era do mercado financeiro digital. As criptomoedas tornaram-se

populares após o boom dos Bitcoins. Tal como a internet a aplicação de recursos financeiros pelo meio digital e, ainda, em moedas digitais, tornou-se acessível. Dessa forma, o mercado passou a oferecer outros e cada vez maiores tipos de aplicações.

Assim, os objetivos do presente trabalho são demonstrar a relação entre o avanço digital e a utilização das moedas digitais como aplicações financeiras, bem como, a falta de regulamentação e o oferecimento de produtos de investimentos com riscos ainda maiores, utilizando do próprio sistema financeiro para constituir crimes digitais, que, apesar de não serem especificamente tipificados, já são configurados crimes contra a ordem financeira, no quesito genérico.

Para alcançar esses objetivos, buscou-se estudar os casos práticos noticiados, da crescente adesão da população brasileira na aplicação financeira em moeda digital e artigos científicos que discutem sobre os crimes digitais.

2 CRIMES DIGITAIS

Com o avanço da sociedade, não seria diferente que o setor tecnológico sofresse com a criminalidade, uma vez que nelas estão presentes de forma globalizada e democrática todos os usuários que constituem a sociedade atual.

A densidade populacional aumentou e proporcionalmente a criminalidade também. O que não ocorreu foi o aumento geográfico, não conquistamos novos territórios terrestres, mas a expansão de seu na via digital, desta forma corrobora CRESPO (p. 27, 2011):

> "Se até a terminologia se alterou, não podia ser diferente com a criminalidade. Esta também encontrou novas formas de se fazer presente, até porque, em alguns casos, há lacunas da lei penal, e como não pode haver analogia in malam partem, há condutas certamente prejudiciais, mas que não são ainda tipificadas como delito [...]"

E, avança no quesito criminalidade, quando indica que "a ética relacionada à tecnologia é quase inexistente, e os criminosos exploram lacunas legais para se manterem ilesos" sendo uma enorme problemática para a sociedade pós-industrial.

2.1 Zona de confiança

Demorou até que a sociedade pudesse estabelecer uma relação confortável com os avanços tecnológicos. Tamanha foi à vontade, que atualmente, confiam-se mais nos dispositivos tecnológicos que em seus pares, seres humanos. Assim, a relação mutualista entre os aparelhos eletrônicos, a internet e demais tecnologias invadiu todas as áreas da vida da sociedade, entre elas, uma zona sempre crítica, a área financeira.

Não faz muito tempo que a sociedade começou a adquirir bens de consumo pela internet e verificar um nível cada vez mais elevado de confiança em uma inteligência artificial. Hoje, a facilidade de utilizar a tecnologia para tudo se estendeu às instituições bancárias e suas funcionalidades.

3 O MERCADO FINANCEIRO

O mercado financeiro precisou se adaptar às mudanças sociais, entre elas, a integração da tecnologia para adequação e atração de novos clientes, cada dia mais aptos aos sistemas informatizados. Assim, foram desenvolvidos diversos softwares para soluções em tecnologia no mercado financeiro, inclusive.

Em detrimento disso, surgiram algumas facilidades também para os criativos criminosos e ambiciosos que se aproveitam da situação para gerar possibilidades entre as lacunas legais para oferecer condições aparentemente vantajosas para novos "consumidores".

3.1 As criptomoedas

O mercado não deixa de ser extremamente promissor, uma grande evolução para a sociedade moderna e faz jus aos desafios e avanços que toda sociedade busca, especialmente no desenvolvimento econômico de um país.

Há diversas variações de criptomoedas e as complicações advém desse conjunto de informações e desinformações. Além disso, da capacidade até então adaptada de se ler a tecnologia em questão.

> O blockchain é uma inovação tecnológica de alcance bem mais amplo que as chamadas criptomoedas que nele se

> baseiam e tem potencial para transformar extensivamente os sistemas de pagamentos e o conjunto das práticas do sistema monetário e financeiro. O desdobramento mais conhecido são as criptomoedas, adjetivo que destaca a utilização de técnicas que permitem proteger dados transmitidos e armazenados de forma descentralizada. A mais utilizada das criptomoedas, o bitcoin, mostra que não se trata de uma moeda em sentido rigoroso, pela ausência das funções de padrão de preços e de reserva de valor e pelo uso muito limitado como meio de pagamento [...]

O autor comtempla as principais fontes que se tornaram investimentos rentáveis e promessas de lucros justos, haja vista a competitividade dos investimentos bancários comuns.

Com receio de ficar para trás, diversos cidadãos embarcaram conhecendo de forma rasa esta fonte de investimento. Confiando muitas vezes da ausência de regulamentação e na boa prática tecnológica, introduziram pouco a pouco as criptomoedas nas suas vidas.

Nesse sentido, PEREIRA; SILVA (2019), concordam que

> "[...] O Bitcoin é a moeda mais proeminente e negociada, tendo sido já aceita como forma de pagamento na compra de apartamentos, carros e em uma crescente gama de outros produtos. Sucede que também já se mostraram viáveis suas possíveis finalidades relacionadas a lavagem de dinheiro, fraudes e ocultação de patrimônio ilícito, cabendo uma análise do entendimento da Polícia Federal e Receita Federal acerca do uso das criptomoedas."

Variação histórica do preço da Bitcoin (2013 a 2017)

Fonte: CoinDesk (2017, on line)

A crescente é nítida, o processo de utilização da moeda digital, não. Não para todos, assim surge algumas margens para a criação de empresas que aproveitam essa oportunidade como faixada de investimentos fraudulentos e o sistema de pirâmide nada moderno.

No sentido da complexidade do investimento, explica ANDRADE (p.44, 2017)

> "Enquanto os investidores usam análises fundamentais para avaliar diferentes classes de ativos, como ações e moedas fiduciárias, investimentos multimercado, tesouro direto e renda fixa, o uso desta abordagem para avaliar a bitcoin é mais complexo, porque não há curvatura de balanço ou números de receitas e ganhos a longo prazo que torne possível desenhar um panorama ideal dos riscos; o que torna a escolha do momento propício para comprar ou vender algo quase que intuitivo."

4 CRIMES DIGITAIS E AS CRIPTOMOEDAS

ANDRADE entende que a utilização de bitcoins atrai agências de aplicação da lei entre outros agentes, que tentam perceber as funcionalidades das criptomoedas e se estão contempladas aos modelos de regulação existentes.

No entanto, apesar de toda discussão em volta do assunto em diversos países "no Brasil, o Banco Central ainda não possui um posicionamento definitivo quanto às negociações com bitcoins, o que demonstra que a instituição ainda não reconhece a relevância dessa tecnologia para o sistema financeiro brasileiro". [1]

Ainda, apresenta o contexto em que cada vez com mais frequência tem sido um cenário de identificação por parte das autoridades no combate ao crime nestes espaços virtuais, de forma que, crimes como a lavagem de dinheiro estão ganhando espaço no que seria um desenvolvimento benéfico na vida financeira das pessoas.

Muitas delas, vítimas de uma falsa ilusão de nova oportunidade, investimento qualificado pelo fato da informatização e da tecnologia, que ainda representa avanço e modernismo, perdem quantias significantes pela dificuldade de monitoramento e pela característica do investimento.

[1] ANDRADE, Mariana Dionísio de. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. **Revista Brasileira Políticas Públicas,** Brasília, v. 7, nº 3, 2017 p. 43-59 54

Na esteira, ANDRADE (p.67, 2017) completa:

> "Com o crescimento dos acessos à internet, as possibilidades de lavagem de dinheiro mudaram e transformaram significativamente cada uma das etapas tradicionais do delito, uma vez que as redes digitais permitem a manipulação do dinheiro lavado a partir de transações com instituições financeiras e empresas legais. A lavagem de dinheiro (ou branqueamento de capitais) não é um fenômeno novo. Os fundos ilícitos foram lavados por muitas décadas, forçando organizações internacionais, governos nacionais e setores privados a empreenderem esforços para enfrentar o movimento ilícito de dinheiro e sua transformação em dinheiro legal. Há três etapas do processo a serem consideradas: depósito de dinheiro no sistema financeiro; distorção da origem do dinheiro por meio de transações lícitas e integração dos valores a setores legais. Diferentes ferramentas já foram desenvolvidas para monitorar e detectar dinheiro suspeito em cada etapa do sistema bancário tradicional, entretanto, no sistema virtual, a criptografia de dados ajuda a esconder as manipulações [...]"

5 CONCLUSÃO

O estudo permitiu compreender que o desenvolvimento é de extrema importância, bem como os avanços legislativos para contemplar a modificação e modernização da sociedade. Ainda que o legislativo não tenha conseguido suprir as lacunas que a atual conjuntura necessita, é preciso haver uma ampla divulgação do assunto para que aos menos as pessoas estão cientes dos riscos que correm.

Não há definição de enquadramento como direito consumerista ou similar. Também não temos certeza se nossas autoridades estão capacitadas para se adequar aos avanços destas empresas privadas que vendem novas possibilidades como fachada de velhos hábitos criminosos. Cedo ou tarde será necessário se adequar, até lá, será um investimento de grande risco, esperar a manifestação dos legisladores pela regulamentação e aos que se arriscam em habitar neste universo dual.

REFERÊNCIAS

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011

ANDRADE, Mariana Dionísio de. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. **Revista Brasileira de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 43-59 54

PEREIRA, Welder Romão; SILVA, Ricardo da Silveira. **Criptomoedas e atuação do estado ao combate de ilícitos**. UNIVERSIDADE CESUMAR. 2019.

CAMPOS, Emília Malgueiro. **Criptomoedas e Blockchain**: o Direito no mundo digital. 2ª Tiragem - Rio de Janeiro: Lumen Juris, 2018.

MARTINS, Pedro**. Introdução a Blockchain**: Bitcoin, Criptomoedas, Smart Contracts, Conceitos, Tecnologia, Implicações. Lisboa: FCA – Editora de Informática, 2018.

CARVALHO, Carlos Eduardo; PIRES, Desiree Almeida; ARTIOLI, Marcel; OLIVEIRA, Giuliano Contento de. Bitcoin, criptomoedas, blockchain: desafios analíticos, reações dos bancos, implicações regulatórias. In: FÓRUM LIBERDADE ECONÔMICA, 0., 2017, São Paulo. **Trabalho.** São Paulo: Mackenzie, 2017. p. 1-23. Disponível em: https://www.mackenzie.br/fileadmin/OLD/62/ARQUIVOS/PUBLIC/SITES/ECONOMICA/2017/Carvalho__Pires__Artioli__Oliveira_-_Bitcoin__criptomoedas..._Encontro_Mackenzie.pdf. Acesso em: set. 2021

CRIMES CIBERNÉTICOS: ESTELIONATO VIRTUAL

Maycon Douglas de Miranda Silva[1]

RESUMO

O presente artigo almeja analisar o estelionato virtual, sua tipificação e as recentes alterações propiciadas pela Lei Ordinária nº 14.155/2021 no Código Penal e no Código de Processo Penal acerca do referido crime, a fim de investigar se tais modificações compreendem um avanço da legislação brasileira em torno dos crimes virtuais. Nesse contexto, também será debatida a figura do comércio eletrônico, o qual possui relevante expressão, pois é considerado o intermediador mais utilizado na contemporaneidade para violar o patrimônio dos usuários da web por criminosos. Na seara jurídica, o tema se mostra relevante pois as recentes alterações relativas à aplicação do Código Penal nos crimes virtuais ainda são palco de muita insegurança jurídica. Para a sociedade, o estudo possui relevância ao promover um entendimento claro sobre o assunto, as formas de prevenção e a recente inclusão do estelionato virtual pela novel Lei nº 14.155/2021, legislação essa que ainda é pouco conhecida socialmente e seus efeitos para aqueles que realizam o crime e para as vítimas ainda são obscuros. O método de estudo a ser utilizado no presente estudo pode ser compreendido como bibliográfico e quanto ao procedimento utilizado é o dedutivo, com o fim de aprimorar as ideias ou descobrir intuições sobre o objeto de estudo.

Palavras-chave: Estelionato virtual. Comércio eletrônico. Lei nº 14.155/2021. Código Penal.

ABSTRACT

This article aims to analyze the virtual embezzlement, its typification and the recent changes provided by the Ordinary Law No. 14.155/2021 in the Criminal Code and in the Criminal Code regarding the aforementioned crime, in order to investigate whether such changes comprise an advance in Brazilian legislation around cybercrime. In this context, the figure of electronic commerce will also be debated, which has relevant expression, as it is considered the most used intermediary nowadays to violate the property of web users by criminals. In the legal area, the theme is relevant because the recent changes related to the application of the Criminal Code in virtual crimes are still the scene of a lot of legal uncertainty. For society, the study is relevant as it promotes a clear understanding of the subject,

[1] Acadêmico de Direito pelo Instituto CEUB de Pesquisa e Desenvolvimento do Centro Universitário de Brasília – UniCEUB – contatomaycon@gmail.com

forms of prevention and the recent inclusion of virtual embezzlement by the novel Law No. 14.155/2021, legislation that is still little known socially and its effects for those who carry out the crime and the victims are still little known. The study method to be used in this study can be understood as bibliographical and the procedure used is deductive, in order to improve ideas or discover insights about the object of study.

Keywords: Virtual embezzlement. E-commerce. Law No. 14,155 / 2021. Criminal Code.

1 INTRODUÇÃO

A internet, atualmente, é a forma mais utilizada mundialmente para a realização de afazeres diários, todavia, alguns indivíduos a utilizam no cometimento de crimes cibernéticos, dentre estes, verifica-se a figura do estelionato virtual. O referido delito é somente uma nuance dessa vertente e merece cuidados, pois o comércio eletrônico está se tornando um instrumento muito usado pelos usuários atualmente e está sendo cada vez mais difundido para a realização de negociações e transações no plano digital, o que gera, também, interesse dos criminosos no âmbito.

O supracitado tem justifica-se, no meio jurídico, em virtude das recentes alterações ocasionadas pela Lei Ordinária nº 14.155/2021 no Código Penal e no Código de Processo Penal no crime de estelionato, inserindo-se a modalidade virtual na tipificação direcionada ao crime, sendo enrijecidas as sanções dispostas, a fim de afastar nocividades no meio virtual. Dessa forma, o estudo se concentra na seguinte problemática: as alterações inseridas pela Lei Ordinária nº 14.155/2021 no crime de estelionato se demonstram suficientes para afastar o delito ou ainda há a necessidade de se elaborar uma lei específica?

Baseando-se nas características do estudo, tem-se uma pesquisa bibliográfica, qualitativa e descritiva que foi utilizada para sustentar cientificamente os objetivos da pesquisa. Com uma didática de cunho exploratório, a pesquisa realiza o levantamento bibliográfico, buscando reunir as informações sobre o tema com o propósito de identificar os assuntos relevantes que deem sustentação aos argumentos elencados. Como referencial teórico, o estudo se baseia em autores renomados como Moisés de Oliveira Cassanti (2014), Evandro Della Vecchia (2014), José Augusto Campos Versiani (2016), Rogério Greco (2009) e muitos outros.

A fim de responder o problema disposto, a pesquisa se divide em quatro momentos, onde o primeiro aborda noções introdutórias sobre os crimes virtuais. O segundo capítulo analisa a figura do estelionato, sua tipificação, objeto jurídico, sujeitos e o debate em torno da modalidade virtual. O terceiro momento traz as legislações brasileiras sobre crimes cibernéticos e, por último, as formas de prevenção de tais crimes e as modificações ocasionadas pela Lei nº 14.155/2021, especialmente aquela que insere o estelionato virtual na redação do Código Penal brasileiro.

Como resultados, o estudo verificou que a Lei nº 14.155/2021 propiciou nítidos avanços na legislação pátria em torno dos crimes virtuais, especialmente o estelionato virtual, todavia, tais intercorrências na web são cada vez mais frequentes, elevando-se a necessidade de uma legislação brasileira específica a tais delitos, a fim de melhor dispor determinações sobre tal contexto.

2 CRIMES VIRTUAIS

Desde épocas remotas, o indivíduo sempre buscou desenvolver meios e técnicas para assegurar o manuseio e distribuição de informações. Cumpre ressaltar que a escrita foi a primeira técnica, que, antigamente, era manifestada como forma de controle sobre a administração de domínios territoriais, como já dito, pelo poder estatal nas extensas civilizações. Mesmo a escrita demonstrando nítida evolução, apenas o desenvolvimento científico foi capaz de possibilitar o manuseio de informações, de modo mais efetivo, por meio dos métodos computadorizados que se elevaram a partir do advento informático.

A partir desse contexto, surgiram os denominados crimes cibernéticos, digitais ou virtuais, relevante para apontar os entendimentos doutrinários sobre o assunto, ora vejamos a compreensão de Feliciano:

> Reconheço por criminalidade informática o recente advento histórico-socio-cultural caracterizado pela alta incidência de ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware, software, redes, entre outros).[2]

[2] FELICIANO, Guilherme Guimarães. Informática e criminalidade: parte I: lineamentos e definições. **Boletim do Instituto Manoel Pedro Pimente**l, São Paulo, v. 13, n. 2, set. 2000. p. 42.

Para tanto, também vale destacar a definição trazida por Rossini, que aduz que o crime cibernético poderia ser apontado como aquela conduta típica e ilícita, edificadora de delito ou contravenção, sendo dolosa ou culposa, comissiva ou omissiva, realizada por pessoa física ou jurídica, com a utilização de meios informáticos, em local de rede ou fora dele, e que viole, direta ou indiretamente a segurança informática, que possui como pressupostos "a integridade, a disponibilidade e a confidencialidade."[3]

Da análise dos mencionados conceitos, primeiramente se observa que os referidos englobam tanto os crimes, quanto as contravenções. Em suma, verifica-se que insere ainda as definições de crime doloso, culposo, assim como os comissivos e omissivos. Assim, se existir disposição para o tipo em sua forma culposa, poderá se tratar de crime cibernético, bem como, tais crimes podem se efetivar na omissão do indivíduo, como, por exemplo, uma empresa que hospeda sites e averigua que o ilícito está sendo realizado, quando da inserção de imagens com material pornográfico de menores em sites de sua hospedagem e esta nada faz para vedar tal conduta.

A partir do entendimento de Rossini, extrai-se que os crimes cibernéticos atingem os atos realizados na seara virtual, assim como qualquer conduta que detenha relação com sistemas informáticos. O autor ainda evidencia o seguinte exemplo: "uma fraude em que o equipamento é utilizado como ferramenta do delito, fora da internet."[4]

Sob outro enfoque, é possível aferir que crime cibernético nada mais é do que um fato típico, antijurídico e culpável, momento em que se utiliza um mecanismo determinado para que se realize tal modalidade. Em virtude disso, os crimes cibernéticos são tidos como crimes de meio, ou seja, trata-se de modalidade criminosa realizada apenas no plano virtual.

Nas lições de Roque define crimes cibernéticos do seguinte modo:

[3] ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004. p. 110.
[4] ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004. p. 111.

> O crime virtual é caracterizado por ser uma conduta lesiva, dolosa, à qual pode representar ou não a obtenção indevida de um benefício, contudo cometida, sempre, com o uso de mecanismos de sistemas de processamento ou comunicação de dados. É necessário, todavia, deixar nítido que nem toda conduta lesiva realizada contra ou por meio de computadores será crime informático. [5]

Pela definição acima, observa-se que a doutrina pátria se demonstra divergente, pois alguns doutrinadores compreendem que o conceito engloba delitos dolosos e culposos, assim como os omissivos e comissivos, à medida que outros autores sustentam o entendimento de que trata somente de crimes virtuais aqueles que possuam em seu âmago o elemento dolo. No entanto, cumpre destacar que a doutrina majoritária compreende que estar-se-á diante de um crime de meio, tendo em vista que o agente realiza a utilização de um computador, para alcançar uma finalidade, isto é, a consumação do crime.

3 **ESTELIONATO:** TIPIFICAÇÃO, OBJETO JURÍDICO, SUJEITOS E SUA PRÁTICA NO MEIO VIRTUAL

Advinda do latim stellionatus (de stellius, que quer dizer camaleão, animal que modifica suas cores ao local em que se encontra, para enganar suas presas e predadores), o crime de estelionato se encontra tipificado no sistema jurídico pátrio, sendo abordada sua figura típica na legislação penal em vigência, no qual possui uma definição expressa no caput do dispositivo 171, conforme se verifica:

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.[6]

Nesse intento, é possível aferir que o mencionado tipi penal se elevou apenas a partir do Império (séc. II d.C), apresentado, primeiramente, como um tipo penal genético e subsidiário, que veio a transmutar, já no século seguinte, como a maneira

[5] ROQUE, Sérgio Marcos. **Criminalidade Informática**. São Paulo: Adpesp Cultural, 2007. p. 310.
[6] BRASIL. **Decreto-lei nº 2.848**, de 07 de dezembro de 1940 (Código Penal). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 20 set. 2021.

mais grave de fraude, "concomitantemente com a extorsão, o rapto, o aborto e a exposição de infante."[7]

Em solo pátrio, a tipificação penal do estelionato obteve seu surgimento a partir do primeiro Diploma penal brasileiro, o Código Criminal do Império, publicado no ano de 1830, que já dispunha como pena em seu artigo 265 o trabalho e a multa de 5% a 20% do valor aferido à coisa.[8]

Sendo assim, em conformidade aos estudos de Mirabete e Fabbrini, "existirá o crime de estelionato quando o agente aferir qualquer que seja a forma fraudulenta capaz de conduzir e manter a vítima ao erro, numa falsa sensação de realidade, com o objetivo e alcançar um benefício ilícito patrimonial."[9] Em suma, consistem à definição do fenômeno, a forma fraudulenta, o erro, o benefício ilícito e a lesão patrimonial, os quais, conjuntamente, compõem o estelionato.

No que tange ao objeto jurídico do mencionado crime, é possível aferir que o que se almeja proteger é a violação do patrimônio do indivíduo e, ainda, "a boa-fé, a segurança, a fidelidade e a veracidade dos negócios jurídicos patrimoniais, ainda que esta se apresente de forma secundária, pois o estelionato é um delito contra o patrimônio."[10]

No que concerne aos sujeitos do crime de estelionato, é possível aferir que o sujeito ativo pode ser qualquer indivíduo, sendo viabilizado o complô de esforços e intentos entre agentes, com fulcro no dispositivo 29 do CP, não se impondo para a incriminação do beneficiado, como sustenta Prado, que intervenha materialmente no contexto do delito. É possível, ainda, que o proveito material seja direcionado a terceiro que, em conformidade ao autor, só responde como partícipe ou coautor se for atestada sua má-fé, caso reste averiguado que o terceiro persuadiu o agente a realizar o crime em benefício dele.[11]

---

[7] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Brasport, 2014. p. 36.
[8] BRASIL. **Lei nº 16 de dezembro de 1830**. Manda executar o Código Criminal. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lim/lim-16-12-1830.htm> Acesso em: 21 set. 2021.
[9] MIRABETE, Júlio Fabbrini; FABBRINI, Renato. **Manual de direito penal:** parte geral. v. 1. São Paulo: Atlas, 2006, p. 87.
[10] MIRABETE, Júlio Fabbrini; FABBRINI, Renato. **Manual de direito penal:** parte geral. v. 1. São Paulo: Atlas, 2006, p. 88.
[11] PRADO, Luiz Regis. **Tratado de direito penal brasileiro**. Parte especial, v. 3, 2014.

Acontece que se o terceiro, não participante do estelionato, descobre o mesmo antes de alcançar seu proveito patrimonial e se, mesmo assim, o recebe, este incidirá no crime de receptação, determinado no dispositivo 180 do CP, verificando-se, ainda, se o seu ato foi culposo ou doloso, isto é, se este possuía o conhecimento de que a coisa seria um produto advindo de estelionato.[12]

No que diz respeito ao sujeito passivo, as lições de Bitencourt revelam que pode ser, similarmente, qualquer indivíduo, seja pessoa natural ou jurídica. Ainda, é possível aferir que esse tipo não impossibilita que a vítima do benefício ilícito e da fraude sejam indivíduos diferentes, como no exemplo elencado pelo autor, "onde o trabalhador sofre a fraude, mas quem custeia o prejuízo é seu empregador."[13]

Cumpre frisar que a vítima deve ser pessoa certa e determinada, haja vista que, tratando-se de indivíduos indeterminados (como na situação de se relevar um mercado eletrônico fraudulento, mas que não possui a ocorrência de vítimas consolidadas ainda) pode se caracterizar crime contra a economia nacional ou contra as relações consumeristas, a depender do caso.

Além de certo e determinado, é necessário aferir que esse indivíduo precisa possuir capacidade de discernimento, pois não há que se mencionar crime de estelionato quando a vítima for incapaz. Caso a vítima se enquadre em tal contexto, caracterizar-se-á o crime de abuso de incapaz, disposto no artigo 173 do CP. Se a vítima não possuir, portanto, ao menos condições de ser ludibriada, configurar-se-á o crime de furto, com fulcro no artigo 155 da legislação penal.[14]

Por sua vez, o estelionato realizado no plano virtual encontra respaldo no já elucidado dispositivo 171 do CP brasileiro. Tal crime, também reconhecido como estelionato digital ou virtual, é um tipo penal no qual o agente se vale de uma forma de comunicação virtual, como a internet, para alcançar a sua finalidade de obter para si benefício patrimonial ilícito, conduzindo ou mantendo a vítima em erro.[15]

---

[12] BRASIL. **Decreto-lei nº 2.848**, de 07 de dezembro de 1940 (Código Penal). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 20 set. 2021.

[13] BITENCOURT, Cezar Roberto. **Tratado de direito penal**: parte especial 5. Saraiva Educação SA, 2016. p. 228.

[14] Ibidem. p. 230.

[15] BRASIL. **Decreto-lei nº 2.848**, de 07 de dezembro de 1940 (Código Penal). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 20 set. 2021.

Essa modalidade criminal pode ser realizada tanto por um especialista na área digital quanto por um leigo que tenha o mínimo de conhecimento possível sobre tal área. Um dos modos de se realizar esse delito é por meio da transferência de montantes via internet, efetuada por vítimas para a conta do delinquente, quando as mesmas são ludibriadas através de falsas páginas na internet, como é o caso da simulação de um site de instituição financeira, por exemplo. Existe ainda a possibilidade de realizar o estelionato por meio de mensagens virtuais enviadas para o e-mail da vítima, na qual convidam os indivíduos a transferirem um determinado valor em dinheiro para a participação de sorteios, com o entendimento de que isso lhe renderá bons frutos.

Nesse diapasão, cumpre destacar o entendimento do Superior Tribunal de Justiça sobre o tema, que por meio do Agravo Regimental CC 74.255-SP proferiu entendimento de que o saque fraudulento efetuado na conta corrente da Caixa Econômica Federal caracteriza o crime de furto mediante fraude, e não estelionato. Na fraude de furto, existiria a diminuição do monitoramento da vítima para que ela não compreenda estar tendo seu patrimônio retirado. Por seu turno, no estelionato, o delinquente procura conduzir e deixar a vítima em erro, para que, dessa forma, ela forneça o bem espontaneamente.[16]

Dessa forma, as lições de Delmanto explanam que:

> Para que seja estelionato é preciso o emprego do artifício ardil, induzir a vítima em erro, obtenção da vantagem ilícita, prejuízo alheio. Assim se faz que com duplo resultado, vantagem ilícita e prejuízo alheio, conexo com a fraude e o erro que provocou.[17]

Atualmente se demonstra frequente que, em compras online ou em paramentos realizados na internet, se exija o preenchimento de formulários, situação essa que trouxe simplificações para indivíduos que não possuem tempo para sair de casa, permeando entre uma loja e outra, dessa forma, estes se valem dos diversos

[16] BRASIL. Superior Tribunal de Justiça. **AgRg no CC: 74225 SP** 2006/0235921-8, Relator: Ministra Jane Silva, Data de Julgamento: 25/06/2008. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/790869/agravo-regimental-no-conflito-de-competencia-agrg-no-cc-74225-sp-2006-0235921-8 > Acesso em: 23 set. 2021.

[17] DELMANTO, Celso et al. **Código penal comentado**. Rio de Janeiro: Ed. Renovar, 2002. p. 396.

instrumentos virtuais que existem, a fim de alcançar a facilidade de fazer compras ou realizar pagamentos em qualquer lugar do mundo.[18]

Nesse sentido, aos indivíduos que se valem de softwares de espionagem para obter benefício ilícito e alcançar os dados pessoais, como e-mails, links, solicitações cadastrais, páginas falsas, dentre outros, acabam conduzindo a vítima ao erro e ao fornecimento de dados pessoais e bancários, e para que mais indivíduos caiam na fraude são realizados inúmeros tópicos e assuntos na intenção de alcançar um amplo número de pessoas. Assim, como exemplo, verificam-se os antivírus, avisos judiciais, cartões de crédito, e-commerce com promoções em sites, dentre inúmeros outros.

Assim, percebe-se que o estelionato virtual pode ser realizado por um indivíduo que possua vasto conhecimento informático, como também pode ser efetuado por indivíduo de pouco conhecimento. O usuário de muito conhecimento almeja inventar formas fraudulentas hábeis a enganar muito bem as suas vítimas, sendo estes denominados crackers, com o objetivo de enganar suas vítimas, "invadindo e realizando atos sem autorização, de forma danosa e ilícita."[19]

O advento tecnológico oferta diversas vantagens e está cada vez mais difundido e acessível ao nosso cotidiano, tendo em vista que toda a sociedade vem aderindo à internet como um instrumento que gera facilidades. A mencionada tecnologia deve sobretudo desencarregar os indivíduos de complexidades diárias, como, por exemplo, o esforço de uma pessoa se locomover até um estabelecimento em busca de um produto desejado, elementos como deslocação e transido durante o percurso até a loja são considerados elementos relevantes que aferem uma evidência maior ao comércio eletrônico.

Frequentemente é possível se deparar com determinado produto na internet e constatar que o valor oferecido nos estabelecimentos físicos se encontra acima aos das lojas virtuais, mesmo que seja apresentado pela mesma empresa, pois existem fatores que influem nesse quesito.

[18] DELMANTO, Celso et al. **Código penal comentado.** Rio de Janeiro: Ed. Renovar, 2002. p. 397.
[19] CRESPO, Marcelo Xavier de Freitas**. Crimes Digitais**. São Paulo. Ed Saraiva. 2011. p. 59.

Dessa forma, o comércio eletrônico é um fenômeno que comporta comodidade ao indivíduo, desde o advento da internet. Com a promulgação do Marco Civil da Internet (Lei nº 12.965/2014) o qual dispõe sobre a utilização da internet no país, surgiu em benefício do empresário que almeja ampliar seu empreendimento, à medida em que se instauram no plano virtual. Todavia, tal mecanismo não se restringe apenas ao horizonte do empreendedor, partindo também ao enfoque do consumidor.[20]

Em suma, é possível verificar que o e-commerce demanda uma logística ágil e prática para simplificar o autoatendimento dos consumidores. Muito distinto ao dos estabelecimentos físicos e essa distinção significativa ocorre em razão de o comércio eletrônico não arcar os mesmos elementos de gestão que um local físico tem de custear com uma maior quantidade de funcionários que se dividem entre as determinadas funções do negócio, por exemplo.

Outras características que distinguem o e-commerce do comércio tradicional são os elevados débitos trabalhistas, como é o caso de alugueis, pois um estabelecimento físico demanda um extenso espaço para estoque e atendimento ao público. Tal fato acarreta impostos maiores e, tendo em vista que o estabelecimento risco possui mais chances de roubos e furtos, existe a necessidade de uma segurança efetiva, fazendo com que os preços se tornem mais baixos em ofertas perpetradas na internet.

Tendo em vista a conjuntura explanada no âmbito virtual, diversas são as práticas criminosas nos meios eletrônicos, ainda mais pelo fato de o mercado eletrônico ter ganhado muita relevância por sua credibilidade de acesso a informações cadastrais de consumidores e dados de cartões de crédito. As mencionadas informações podem ser extraídas através de vírus infiltrado na conta de e-mail ou ainda uma conexão de wi-fi estranha, permitindo a coleta de senhas salvas no equipamento, que podem ou não nortear a um ambiente de compras virtuais. Esse impasse vem gerando cada vez mais adversidades aos consumidores digitais.

[20] BRASIL**. Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 23 set. 2021.

O estelionato e a fraude permeiam de modo similar em tais situações, todavia existe uma distinção entre ambos. Greco aduz que ambos não se confundem, em observância ao elemento comum de defraudar, na fraude, o cibercriminoso age para diminuir a vigência da vítima aos poucos sobre o bem almejado. Por seu turno, o estelionato é o meio usado para que o criminoso convença a vítima a ser conivente com a conduta, aferindo a ela uma falsa noção sobre o que está ocorrendo.[21]

Portanto, conclui-se que a internet, apesar de gerar facilidades, também aferiu determinado encorajamento aos criminosos, que costumam se esconderem atrás do anonimato alcançado no plano virtual. Atualmente, o crime de estelionato possui uma questão agravante muito nítida na seara digital, ao passo que o estelionatário determina quanto quer tirar de um indivíduo e de quantos irá tirar ao mesmo tempo, bastando somente um clique, utilizando-se de meios tecnológicos que lhe aferem o almejado anonimato, seja mascarando o IP do computador ou se utilizando de wi-fi e equipamentos alheios.

4 LEGISLAÇÃO NACIONAL SOBRE CRIMES CIBERNÉTICOS

Inicialmente, vale frisar que como uma forma de simplificar e até mesmo viabilizar as investigações dos crimes cibernéticos foram efetuadas algumas iniciativas de leis no Brasil. Assim, verificam-se as leis dos Cyber cafés, regras estas que estabelecem a guarda dos registros de acesso dos indivíduos pelos locais que viabilizam o acesso à internet. No momento de criação das mencionadas leis, em meados de 2006, vislumbrou-se um certo impasse, em razão da recorrente justificativa de censura e vigilância inadequada, acepções essas que não são mais sustentadas devido aos riscos à segurança observados na internet.[22]

Nesse sentido, constatou-se uma escolha entre liberdade irrestrita no acesso anônimo ilimitado na internet ante à garantia de um determinado rastreamento de cibercriminosos que se valem dos meios tecnológicos para prover danos aos

[21] GRECO, Rogério. **Curso de direito penal.** 11ª ed. Niterói: Impetus, 2009. p. 99.
[22] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014. p. 89.

indivíduos de maneira mais conveniente. Felizmente, a primeira opção está sendo assentada mesmo que timidamente.

Por sua vez, a Lei nº 12.735/2012, reconhecida como Lei Carolina Dieckmann, foi promulgada em decorrência do crime virtual envolvendo a atriz por meio de uma violação de dados digitais. A atriz teve seu computador invadidos por cibercriminosos, reconhecido por serem especialistas no âmbito informático, após revelados conhecimentos e habilidades no tocante ao âmbito, se distinguindo dos demais hackers pela sua utilização norteada de modo antiético.[23]

Os criminosos disseminaram na rede algumas imagens íntimas da atriz em decorrência do fato de não receberem a quantia de R$ 10.000,00 pedida à Carolina para a conservação e sigilo de tais fotos. Essa situação, além da interceptação de e-mail, caracterizou o crime de extorsão. Através da Lei nº 12.735/2012, foi inserido ao artigo 154 do CP a disposição de crime de invasão de dispositivo de terceiro, sem razão ou consentimento do indivíduo, com pena de três meses a um ano de reclusão, com majorante, caso a referida invasão afira danos econômicos à vítima ou se trate da Administração Pública no polo passivo da demanda.[24]

A mencionada lei, apesar de ter sido considerada um mecanismo de avanço no Brasil, ainda mais se observarmos a existência de tal disposição sobre a invasão de dispositivos tecnológicos, ainda é muito tímida. Basta observar a intensidade danosa de uma invasão a um aparelho informático que possua informações ou dados íntimos de algum indivíduo.

Assim, não se mostra infrequente a realização de suicídios decorrentes de uma divulgação inadequada de dados pessoais, o que vulnerabiliza o indivíduo de tal maneira, que o prejuízo pode ser considerado irreparável. Existe uma determinada limitação no que tange à proteção da imagem e da honra dos indivíduos por meio da legislação penal, e tal fato fica ainda mais nítido atualmente, em razão da disseminação e intensidade dos crimes realizados no plano virtual.

---

[23] BRASIL. **Lei nº 12.735**, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 23 set. 2021.
[24] Ibidem.

Uma questão que suscita críticas é o fato de a norma ter criminalizado somente a invasão para alcance de vantagem indevida, não incluindo desse modo o caso de um delinquente que queira somente ver informações do indivíduo, mesmo sem a finalidade de obter alguma vantagem diretamente. Assim, o que nos resta aferir sobre a conduta de uma pessoa que acessa a conta pessoal de alguma rede social de outrem que esqueceu a mesma aberta? Como não existiu violação inadequada da segurança, a conduta seria considerada atípica, o que nos leva ao questionamento sobre a generalidade de tal dispositivo.

Outra questão relevante a ser evidenciada é a força da influência midiática exercida no Brasil, que de determinado modo foi tão decisiva para a promulgação da Lei nº 12.735/2012, que nos passa o sentimento de que a vida pessoal de uma pessoa famosa talvez seja mais relevante que a segurança da informação a um desconhecido. Em nosso país existe a intensa tendência de se repercutir nacionalmente para a elaboração de leis quando ocorrem fatos de grande mobilidade social, como exemplo da Lei Carolina Dieckmann.[25]

Por seu turno, a Lei nº 12.965/2014, reconhecida como o Marco Civil da Internet (MCI), compreende uma relevante ferramenta para o combate aos crimes cibernéticos. A referida lei consiste em uma colaboração para a investigação de delitos cibernéticos, e almeja por meio da disposição de princípios e garantias tornar o ambiente virtual mais seguro e menos hostil. O MCI também procura conservar a harmonia e o equilíbrio entre a liberdade de expressão e a transmissão de informações com determinações de segurança, como é o caso da responsabilidade civil direcionada aos provedores de internet e usuários.[26]

O MCI é comportado em três premissas, quais sejam: a segurança da neutralidade da rede, a proteção à privacidade aferida aos usuários da rede e o direito à liberdade de expressão. A neutralidade almeja assegurar que as operadoras não cobrem de modo distinto a depender do material que circula na web, podendo a

[25] BRASIL. **Lei nº 12.735**, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 23 set. 2021.

[26] BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 23 set. 2021.

mesma cobrar somente em observância às velocidades ofertadas. O mencionado instrumento almeja consolidar uma democratização do acesso à internet.

Sobre a privacidade do usuário, segundo Lisboa e Lopes, "o diploma procura respaldar os dados dos usuários junto aos provedores, de forma que somente em casos especiais possa existir uma quebra do sigilo de tais dados."[27] Assim, é possível evidenciar que não existem direitos absolutos, e que em determinadas situações um direito pode ser relativizado, tendo sobretudo disposições constitucionais sobre o assunto.

É possível aferir que a regulamentação do MCI foi benéfica pois englobou a determinação de prazos mínimos para a conservação de registros de acesso e conexão, além da exigência de observância da legislação nacional para condutas efetivadas em território brasileiro. Sob outro viés, a sensação que se estabelece é que o MCI tenta proteger os indivíduos das ameaças à liberdade e à vida privada quando realizadas pelo ente estatal, o que fundamenta a precisão de ordem judicial para obtenção de registros. Desse modo, é como se o Estado fosse o maior interessado em violar a privacidade dos indivíduos, ocorre que tal ordem judicial acaba por acarretar mais burocracias e protelar investigações.

Assim, verifica-se que o alcance de dados de registro é indispensável até mesmo para o estabelecimento dos melhores caminhos de investigação, e morosidades desnecessárias são obstáculos encontrados na identificação do delinquente, que comumente se encontra em passos à frente dos policiais.

Por fim, a perícia digital consiste em um exame técnico operado por especialista em dados digitais, tendo tal profissional o encargo de verificar os assuntos relativos ao hardware e ao software de meios tecnológicos, como computadores, notebooks, celulares, tablets, dentre outros. Nesse intento, incisivas são as palavras de Vecchia (2014, p. 77), que aduz:

> A perícia digital se vale de um emaranhado de técnicas e procedimentos com fundamento científico para coletar, analisar e apontar as evidências encontradas. Possui a

[27] LISBOA, Cícero de Barros; LOPES, Gustavo Matias. **Os Três Pilares do Marco Civil da Internet**. Disponível em:<http://periodicoalethes.com.br/media/pdf/5/os-tres-pilares-domarco-civil-da-interne.pdf> Acesso em: 24 set. 2021. p. 83.

> finalidade de alcançar informações referentes a casos passados em uma investigação (não somente no âmbito criminal ou cível, como também em ocorrências particulares nas quais não se deseja acionar a polícia ou o judiciário, em um primeiro momento. Através da análise dos fatos ocorridos, é possível recompor as condutas realizadas nos diversos equipamentos e mídias questionados.[28]

Insta frisar que na perícia digital os indícios encontrados são constituídos geralmente de modo indireto, isto é, no caso de um equipamento tido como suspeito ter sido usado para a realização de algum ilícito, qualquer programa ou arquivo irá aferir um vestígio de tal ocorrência indiretamente, ao contrário dos delitos realizados fora do plano virtual, onde um indício precisa somente ser interpretado, como um fio de cabelo encontrado nas unhas de uma vítima de homicídio, por exemplo, que leva a considerar uma luta antecedente com o agressor.[29]

Todavia, vale ressaltar que a conjuntura de perícia digital apesar de se encontrar em contínua evolução, ainda necessita de muitos desenvolvimentos para que o combate aos delitos cibernéticos possa ser realmente efetivado. Dessa forma, o número de peritos digitais no Brasil ainda é muito escasso, o que é capaz de obstaculizar o decurso de investigações para tais delitos que crescem cada vez mais no país e no mundo.[30]

Portanto, conclui-se que o Brasil necessita em caráter de urgência elaborar uma lei específica para os delitos cibernéticos, ainda mais levando em consideração que a internet atualmente é essencial para a sociedade. Assim, se faz indispensável no sistema jurídico nacional uma tipificação mais ampla sobre as condutas ilícitas realizadas na web. O Estado nacional ainda se demonstra muito atrasado no tocante à tais legislações específicas, sendo vislumbrada a necessidade de afastar a ocorrência desmedida de tais crimes.

---

[28] VECCHIA, Evandro Della. **Perícia Digital**: Da Investigação à Análise Forense. Campinas: Millenium, 2014. p. 78.

[29] VECCHIA, Evandro Della. **Perícia Digital**: Da Investigação à Análise Forense. Campinas: Millenium, 2014. p. 79.

[30] COSTA, Marcelo Antônio Sampaio Lemos. **Computação Forense**. Campinas: Millenium, 2011. p. 102.

5 A PREVENÇÃO DOS CRIMES VIRTUAIS E AS ALTERAÇÕES PROPICIADAS PELA LEI Nº 14.155/2021 NO CRIME DE ESTELIONATO

O advento dos meios tecnológicos propiciou aos indivíduos uma visível facilidade e, em contrapartida, a dependência de seus usuários, seja no labor, em casa ou em qualquer local onde seja admitido sua utilização indiscriminada. Nessa perspectiva, o e-commerce edificado para simplificar a vida destes indivíduos apresenta possíveis ameaças, como é o caso do estelionato virtual, objeto da presente pesquisa.

Elevadas tais questões, verifica-se a necessidade de promover instrumentos protetivos e preventivos aos abusos realizados na internet. Tutela essa baseada no ato ou efeito se resguardar de algum dano ou delito que possa vir a se realizar. A prevenção almeja impedir que o delito ocorra, efetuando ações com finalidade de colocar empecilhos no caminho da violência e delinquência, tendo em vista que não existe uma maneira de assegurar totalmente a ocorrência de tais crimes.[31]

Com o objetivo de preservar os dados e seu equipamento de ameaças virtuais, os usuários de grandes redes devem se prevenir com a utilização de todos os meios viáveis e à disposição contra os crimes cibernéticos. A fim de transpassar uma possível alternativa ao combate do estelionato virtual, o estudo passa a explanar alguns instrumentos preventivos contra a realização de crimes virtuais.

Inicialmente, o primeiro modo de prevenção seria a utilização de senhas, onde o indivíduo faz utilização de informações pessoais para validar o acesso a sistema de informação de locais de uso pessoal, como, por exemplo, aplicativos de bancos, e-mails, transações via internet, dentre outros. Em conformidade aos estudos de Zaniolo, algumas precauções devem ser levadas em consideração na criação de senhas, como, por exemplo, "não estar contida em dicionários, idiomas estrangeiros ou assentos correlatos, não utilizar elementos como dia e mês de aniversário, sobrenome, apelidos, dentre outros."[32]

[31] VALLOCHI, Savio Talamoni. **Tipificação dos Crimes de Informática, métodos de combate e prevenção**. São Paulo: Saraiva Educação. 2004. p. 80.

[32] ZANIOLO, Pedro Augusto. **Crimes Modernos**: o impacto da tecnologia no Direito. Curitiba: Juruá, 2007. p. 363.

Os softwares Antimalware também são outras ferramentas protetivas dos computadores, servindo como instrumentos que almejam constatar e, então eliminar tais arquivos maliciosos do equipamento, dentre estes se encontram os reconhecidos antivírus. É relevante colocar a necessidade ter um software antimalware sempre atualizado, ao passo que é uma medida preventiva contra os denominados malwares, isto é, os programas instalados com o intento de ocasionar algum dano no sistema. Obtendo-se como fundamento tais afirmações que Zaniolo aponta algumas das principais vantagens do software antivírus:

> a) Constatar e extirpar a maior quantidade possível de vírus malware; a) verificar os arquivos advindos através da internet; c) procurar ameaças em arquivos anexados a mensagens de e-mail; d) analisar frequentemente os discos de maneira transparente ao usuário.[33]

É indispensável que o antivírus a ser utilizado seja de boa procedência, para que os sistemas de dados estejam sempre atualizados, e antes de começar qualquer ação no equipamento faça uma inspeção no sistema para que assim possa examinar a presença de possíveis ameaças no computador.

O denominado firewall é um mecanismo de extrema relevância na proteção dos crimes virtuais, Pinheiro o define como sendo um instrumento protetivo da rede interna de uma organização contra possíveis ameaças, hackers mal-intencionados e criminosos que percorrem os caminhos da internet, os mantendo longe do sistema, a fim de isolar os danos nessa seara.[34]

O firewall, quando configurado adequadamente, pode registrar os intentos de acesso aos serviços habilitados no seu equipamento; obstruir o envio para terceiro de dados e informações colhidos por invasores e códigos maliciosos; afastar possíveis invasões e explorações de vulnerabilidades do seu equipamento e viabilizar a constatação das origens de tais tentativas, dentre outras coisas.[35]

Nesse instrumento, se faz essencial o exame da procedência do produto, isto é, se este é confiável, analisar a ativação apropriada do programa e, principalmente

[33] Ibidem p. 366.
[34] PINHEIRO, Patricia Peck. **Direito digital.** 8. ed. rev. atual. e ampl. São Paulo: Saraiva, 2010. p. 255.
[35] CARISSIMI, Alexandre da Silva; ROCHOL, Juergen; GRANVILLE, Lisandro Zambenedetti. **Rede de computadores**. Porto Alegre: Bookman, 2009. p. 122.

buscar registrar a maior quantidade de informações, viabilizando um status máximo de alerta das comunicações de tentativa de invasão.

Ainda, verifica-se os nomeados filtros AntiSpam, que são vinculados às contas de e-mail e programas relativos, viabilizando a divisão de e-mails indesejados, os referidos spams, podendo, dessa forma, o usuário dividi-los conforme seu intento. Por fim, cumpre evidenciar a utilização de honeypots e honeynets, considerados recursos computacionais para a segurança, direcionados à finalidade de enganar um possível malfeitor e fazê-lo pensar que conseguiu a invasão do sistema, quando, verdadeiramente, está em um local simulado, tendo todas as suas ações inspecionadas. [36]

Posto isso, verifica-se que tais precauções são muito bem-vindas para o afastamento de crimes no ambiente digital, todavia, não são o suficiente para dizimar tais delitos, sendo necessária uma legislação específica para tais crimes, como é o caso do estelionato virtual, que alcançou grande avanço através da novel Lei nº 14.155/2021.[37]

A Lei Ordinária nº 14.155/2021 adveio do PL nº 4.554/2020, trazendo algumas modificações no Código Penal e no Código de Processo Penal, com a intenção de enrijecer as sanções aferidas aos crimes de violação de dispositivos informáticos (art. 154-A do CP), furto (art. 155 do CP) e do estelionato (art. 171 do CP) realizados no meio virtual ou de forma eletrônica, assim como de estabelecer a competência para o processamento de algumas formas do estelionato no domicílio da vítima.

Foram três modificações realizadas no crime de estelionato através da Lei nº 14.155/2021. Vejamos a nova redação do art. 171 no que tange ao estelionato virtual:

[36] Ibidem p. 123.

[37] BRASIL. **Lei nº 14.155**, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm> Acesso em: 24 set. 2021.

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
>
> [...]
>
> Fraude eletrônica
>
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
>
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021)
>
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.[38]

Ainda, a Lei nº 14.155/2021 incluiu o 4º ao art. 70 do CPP dispondo sobre o tema. A modificação em comento era muito almejada pois, na legislação anterior, pairava uma forte insegurança jurídica defronte à existência de normas diferentes para casos similares e da oscilação da jurisprudência sobre o assunto.

Segundo o art. 70 do Código de Processo Penal, os crimes dispostos no art. 171 do CP, quando realizados mediante depósito, emissão de cheques sem suficiente provão de fundos em poder do sacado ou com o pagamento frustrado através de transferência de quantias, a competência será estabelecida em observância ao local de domicílio da vítima e, se existirem várias vítimas, a competência será firmada pela prevenção.[39]

Por último, vale mencionar que a Lei nº 14.155/2021 não possui vacatio legis, assim, as modificações propiciadas no CP e no CPP, que buscam aferir maior concretude ao combate dos crimes virtuais, aumentando a abrangência dos ilícitos penais, majorando as penas para tais crimes, assim como determinando a regra de

[38] BRASIL. **Lei nº 14.155,** de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm> Acesso em: 24 set. 2021.

[39] Ibidem.

competência em benefício do acesso da vítima aos órgãos competentes, já se encontram vigentes no ordenamento jurídico brasileiro, representando um nítido – mas ainda tímido – avanço da legislação brasileira no combate aos crimes cibernéticos.

Todavia, ainda que a novel legislação represente um avanço no Brasil sobre os crimes virtuais, cumpre ressaltar que tais ocorrências são cada vez mais frequentes e os cibercriminosos estão frequentemente se atualizando sobre técnicas avançadas para o cometimento de crimes nesse âmbito, demonstrando, assim, a necessidade de uma legislação específica para tais crimes.

6 CONCLUSÃO

Com a realização do presente estudo, verificou-se que a internet se encarregou de propiciar melhorias aos indivíduos, viabilizando conforto, variedades e maior extensão de pesquisas para aqueles que almejam uma análise de preços antes de realizar a compra. Todavia, também foram ocasionados alguns malefícios, ao passo que encorajou criminosos a se esconderem no anonimato da web e o Código Penal brasileiro se viu obrigado a determinar a inclusão do estelionato praticado no ambiente virtual com a Lei nº 14.155/2021, que representou um visível avanço na legislação brasileira sobre o tema.

O estelionato virtual é um ilícito penal no qual o indivíduo se vale de uma forma de comunicação digital, por exemplo, através da internet, para atingir o seu objetivo de benefício patrimonial ilícito, induzindo ou conservando a vítima em erro. Tal modalidade de crime pode ser cometida tanto por um especialista do âmbito digital quanto por um leigo que possua o mínimo de conhecimento sobre o assunto, sendo a transferência de valores via internet uma forma corriqueira para a ocorrência de tal crime.

Observou-se, ainda, que o conhecimento do usuário sobre códigos maléficos como botnet, defacement e trojan se demonstra muito importante por mostrar um caminho para que o investigador ou perito criminal consiga examinar um crime virtual. Assim, tal conhecimento também pode contribuir para a cognição do juiz, que analisará o caso concreto que englobe elementos tecnológicos e, através da

compreensão das referidas ameaças, é possível atingir uma deliberação sobre a extensão dos danos que estas podem causar.

O estudo também trouxe algumas formas de prevenção que os usuários da internet podem investir, como é o caso dos antimalwares, denominados antivírus, capazes de constatar e retirar ameaças com intento de invasão no dispositivo. Por sua vez, o firewall é um mecanismo de extrema relevância na proteção dos crimes virtuais, sendo definido como um mecanismo protetivo da rede interna de uma organização contra possíveis ameaças, hackers mal-intencionados e criminosos que percorrem os caminhos da web, os mantendo longe do sistema, a fim de isolar os danos nessa seara.

O estudo analisou as modificações geradas pela Lei Ordinária nº 14.155/2021, oriunda do PL nº 4.554/2020, que endureceu as sanções aferidas aos crimes de dispositivos informáticos (art. 154-A do CP), furto (art. 155 do CP) e do estelionato (art. 171 do CP), além de incluir a última modalidade realizada no ambiente virtual ou eletronicamente, antes não tipificada, ainda, a novel legislação determinou a competência para o processamento de algumas formas do estelionato no domicílio da vítima.

Portanto, conclui-se que, ainda que a Lei Ordinária nº 14.155/2021 tenha refletido avanços ao incluir a figura do estelionato virtual no Código Penal e endurecer as sanções dos crimes realizados na internet, verifica-se continuamente uma maior frequência de tais crimes, onde os criminosos estão cada vez mais atualizados e munidos de novos métodos para o cometimento de tais delitos, elevando-se, assim, a necessidade de uma legislação específica.

REFERÊNCIAS

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial 5**. Saraiva Educação SA, 2016.

BRASIL. **Decreto-lei nº 2.848, de 07 de dezembro de 1940.** Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 20 set. 2021.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 23 set. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 23 set. 2021.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm> Acesso em: 24 set. 2021.

BRASIL. **Lei nº 16 de dezembro de 1830.** Manda executar o Código Criminal. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/lim/lim-16-12-1830.htm> Acesso em: 21 set. 2021.

BRASIL. Superior Tribunal de Justiça. **AgRg no CC: 74225 SP 2006/0235921-8**, Relator: Ministra Jane Silva, Data de Julgamento: 25/06/2008. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/790869/agravo-regimental-no-conflito-de-competencia-agrg-no-cc-74225-sp-2006-0235921-8 > Acesso em: 23 set. 2021.

CARISSIMI, Alexandre da Silva; ROCHOL, Juergen; GRANVILLE, Lisandro Zambenedetti. **Rede de computadores**. Porto Alegre: Bookman, 2009.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.

COSTA, Marcelo Antônio Sampaio Lemos. **Computação Forense**. Campinas: Millenium, 2011.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo. Ed Saraiva. 2011.

DELMANTO, Celso et al. **Código penal comentado**. Rio de Janeiro: Ed. Renovar, 2002.

FELICIANO, Guilherme Guimarães. **Informática e criminalidade**: parte I: lineamentos e definições. Boletim do Instituto Manoel Pedro Pimentel, São Paulo, v. 13, n. 2, set. 2000.

GRECO, Rogério. **Curso de direito penal**. 11ª ed. Niterói: Impetus, 2009.

LISBOA, Cícero de Barros; LOPES, Gustavo Matias. **Os Três Pilares do Marco Civil da Internet**. Disponível em:<http://periodicoalethes.com.br/media/pdf/5/os-tres-pilares-domarco-civil-da-interne.pdf> Acesso em: 24 set. 2021.

MIRABETE, Júlio Fabbrini; FABBRINI, Renato. **Manual de direito penal**: parte geral. v. 1. São Paulo: Atlas, 2006.

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

PRADO, Luiz Regis. Tratado de direito penal brasileiro. **Parte especial**, v. 3, 2014.

ROQUE, Sérgio Marcos. **Criminalidade Informática**. São Paulo: Adpesp Cultural, 2007.

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

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

VALLOCHI, Savio Talamoni. **Tipificação dos Crimes de Informática, métodos de combate e prevenção**. São Paulo: Saraiva Educação. 2004.

VECCHIA, Evandro Della. **Perícia Digital**: Da Investigação à Análise Forense. Campinas: Millenium, 2014.

VERSIANNI, José Augusto Campos. **Cooperação Internacional na Investigação de Crimes Cibernéticos**. Rio de Janeiro: Mallet, 2016.

ZANIOLO, Pedro Augusto. **Crimes Modernos**: O Impacto da Tecnologia no Direito. Curitiba: Juruá, 2007.

A PROBLEMÁTICA DA PORNOGRAFIA VIRTUAL INFANTIL

Mariana Guimarães Dourado[1]

RESUMO

O presente artigo pretende fazer uma análise acerca da problemática da pornografia infantil virtual. Com o avanço da tecnologia e o crescimento dos ambientes virtuais, além dos diversos benefícios trazidos, vieram também o aparecimento de novos crimes praticados digitalmente, dentre eles está inserida a pornografia infantil. Para entender a abrangência desse crime, será feito um estudo acerca dos crimes digitais e seus principais aspectos e divisões e das legislações como o Marco Civil da Internet, Lei 12.965 de 2014 e a Lei Carolina Dieckmann, Lei 12.737 de 2012, que foram criadas para tentar regulamentar as questões que envolvem o ambiente virtual. Logo após serão abordados os institutos que criminalizam a pornografia infantil, passando pelo Estatuto da Criança e do Adolescente, Lei 8069 de 1990 e pelo Código Penal e a importância dessas leis para assegurar a punição de quem cometer esses delitos, garantindo uma maior proteção para a criança e o adolescente. Assim será entendido como o crime está muito presente nos dias atuais no Brasil e seus números seguem aumentando, como pode ser observado com os índices maiores no ano de 2020, com a pandemia do COVID-19, fazendo-se também a análise de como existem muitas dificuldades para seu enfrentamento. Esse estudo é necessário para se poder chegar a soluções efetivas de enfrentamento dessa prática delituosa, como uma mudança nas leis, uma maior conscientização das crianças sobre os riscos na internet e uma conscientização da sociedade para denúncias e reprimir esse tipo de crime, garantindo assim, a segurança e os direitos fundamentais das crianças e dos adolescentes.

Palavras-chave: pornografia infantil; crimes digitais; crimes contra a criança e adolescente.

ABSTRACT

This article intends to analyze the problem of virtual child pornography. With the advancement of technology and the growth of virtual environments, in addition to the various benefits brought, came the appearance of new crimes committed digitally, including child pornography. To understand the scope of this crime, a study will be made about digital crimes and their main aspects and divisions and

[1]Bacharel e Direito. Pós-graduanda em Direito Penal e Controle Social pelo Centro Universitário UniCEUB; mariana.dourado@sempreceub.com.

legislation such as the Marco Civil da Internet, Law 12.965 of 2014 and the Carolina Dieckmann Law, Law 12.737 of 2012, which were created to try to regulate issues involving the virtual environment. Soon after, the institutes that criminalize child pornography will be addressed, including the Child and Adolescent Statute, Law 8069 of 1990 and the Penal Code and the importance of these laws to ensure the punishment of those who commit these crimes, ensuring greater protection for the child and teenager. Thus, it will be understood that crime is very present in Brazil today and its numbers continue to increase, as can be seen with the higher rates in 2020, with the COVID-19 pandemic, also analyzing how they exist many difficulties to face it. This study is necessary in order to arrive at effective solutions to fight this criminal practice, such as a change in the laws, a greater awareness of children about the risks on the internet and an awareness of society for complaints and repress this type of crime, thus ensuring, the safety and fundamental rights of children and adolescents.

Keywords: child pornography; digital crimes; crimes against children and adolescents.

1 INTRODUÇÃO

A pornografia virtual infantil, com o advento da tecnologia, passou a se fazer mais presente no mundo da internet e seus números se tornaram alarmantes. É certo que a tecnologia e a internet, trouxeram diversos benefícios e facilidades para a vida das pessoas, mas na mesma medida trouxe diversos problemas, como a nova incidência de crimes cometidos por meios digitais.

Dessa forma, crimes que anteriormente já eram cometidos, passaram também a constar em plataformas digitais, aumentando os números de criminalidade. Para regular o ambiente virtual, foram criados institutos como o Marco Civil da Internet e a Lei Carolina Dieckmann, para que a internet não fosse uma terra sem leis e os infratores pudessem responder por suas condutas.

Entretanto, mesmo com essas Leis, o número de pornografia infantil na internet ainda se encontra muito alto, havendo uma dificuldade de se combater esses crimes, pelo fato de existir uma agilidade para seus vestígios serem apagados.

Dessa forma, o artigo procurou trazer essa problemática e as possíveis soluções para que essa incidência de crimes pare de ocorrer. Para isso, o trabalho será dividido em três tópicos.

No primeiro, será feita uma análise acerca dos crimes digitais e como a criação da internet fez com que esses crimes começassem a acontecer, analisando também os importantes institutos de combate a esses crimes

No segundo tópico, será estudado o histórico de criação dos direitos fundamentais e de proteção às crianças e adolescentes, passando também pela análise acerca da pornografia infantil virtual e das leis que tratam de sua criminalização, o Estatuto da Criança e do Adolescente e o Código Penal.

Por fim, no terceiro tópico será estudado a incidência do crime de pornografia infantil virtual no Brasil e como esse crime afeta em muito as crianças e a sociedade, devendo haver mecanismos mais eficientes para que essa problemática seja combatida, como a criação de novas leis, políticas públicas, assistência as crianças e adolescentes e um maior controle acerca dos conteúdos que estão sendo divulgados na internet.

Devendo haver, dessa forma uma junção da sociedade, conjuntamente com o Estado e a jurisdição, para que novas leis e mecanismos possam ser criados para coibir essa prática e para que as crianças possam ter seus direitos fundamentais garantidos, passando a serem devidamente protegidas.

O estudo em questão, será feito por meio de pesquisa bibliográfica e documental, analisando-se a doutrina e a legislação acerca da temática, como o objetivo de desenvolver uma crítica por meio desses fundamentos.

2 DOS CRIMES DIGITAIS

A internet ao longo do tempo se tornou um importante meio de acesso e compartilhamento de informações, passando a mais presente no dia a dia das pessoas, porém apesar dos diversos benefícios e facilidades que a internet ofereceu para a vida das pessoas, foram trazidos novos problemas, conjuntamente, como os crimes cometidos em meios digitais.

A inovação digital proporciona à grande parte de pessoas, uma maior facilidade de acesso ao mundo dos computadores. A cada dia surgem novos dispositivos eletrônicos com o objetivo de facilitar de forma mais abrangente a vida

dos indivíduos e seus negócios, podendo as atividades serem realizadas apenas com um clique. [2]

Os crimes digitais, são os realizados em meios virtuais. O maior incentivo para esses crimes é dado pela ideologia de que o meio digital é um ambiente sem leis, contudo, é importante a compreensão de que a internet é um meio de praticar delitos que podem ser amoldados em tipos penais já existentes. [3]

Porém, devem ser necessárias novas propostas para a dimensão dos delitos na legislação, pois a criminalidade da informática não é apenas um meio para a atuação de condutas já tipificadas, podem existir lesões a bens jurídicos específicos. [4]

No mesmo sentido, os delitos tipificados na lei penal, possuem novas formas de agir pelo fato de o modo de operar ser facilitado pelo anonimato da internet. dessa forma, ofensas como o bullying, delitos sexuais e econômicos representam aspectos alarmantes da sociedade moderna. [5]

O Direito Penal, possui um envolvimento com a informática pois são discutidos assuntos como o acesso não autorizado a sistemas, spam, engenharia social, estelionato, vírus, legítima defesa relativa a ataques em sistemas computacionais, lugar do crime, entre outros. [6]

O conceito de conduta delituosa no meio informático pode ser definido como uma conduta típica e ilícita, podendo ser um crime ou uma contravenção dolosa ou culposa, comissiva ou omissiva, praticada por qualquer pessoa, física ou jurídica, que utilize do computador para agredir direta ou indiretamente a segurança digital. [7]

O crime digital pode ser entendido, também, como um ato de lesividade cometido pelo uso de um computador ou de outro aparelho eletrônico com o intuito

[2] SERRA, Thalyta Maia Galvão. A pedofilia na internet à luz do estatuto da criança e do adolescente. 2009. 86 f. Monografia (Graduação em direito) – FESP Faculdades, João Pessoa. 2009.
[3] CASSANTI, Moisés de Oliveira. "Crimes virtuais, vítimas reais." *Rio de Janeiro: Brasport* (2014).
[4] Crimes digitais/ Marcelo Xavier de Freitas Crespo- São Paulo: Saraiva, 2011.
[5] Crimes digitais/ Marcelo Xavier de Freitas Crespo- São Paulo: Saraiva, 2011.
[6] CRESPO, Marcelo, 2011, P. 45
[7] ROSSINI, Augusto Eduardo de Souza. Informática, Telemática e Direito Penal. São Paulo: Memória Jurídica, 2004.

de se obter uma vantagem indevida, incluindo diversos delitos como roubo, pedofilia, tráfico de drogas e de pessoas, calúnia, difamação, injúria, entre outros. [8]

O ambiente digital é um campo para cometimento de delitos já tipificados no ordenamento jurídico, mas também pode ser um ambiente para condutas que ainda não são incriminadas no Brasil e que podem na mesma medida serem altamente danosas.

Essa situação se dá pela vulnerabilidade desse ambiente pelo fato de possuírem a capacidade de processar, guardar e circular de forma automática e em tempo real, grandes quantidades de informações, pelo grande número de usuários e a frequência com que o acessam, a liberdade para enviar informações, podendo seus usuários se tornarem possíveis vítimas, o fato de que as técnicas e logicas podem ser acessadas de forma ilegítima e ter seu conteúdo alterado e a possibilidade de multiplicação de ações ilícitas, como por exemplo, fóruns de debates, páginas na internet. [9]

A doutrina procurou classificar os crimes digitais em próprios, sendo todas as condutas praticadas contra bens jurídicos informáticos e os crimes digitais impróprios que são os que se dirigem a bens jurídicos tradicionais, não inerentes à tecnologia. [10] Nesse mesmo sentido:

> "Crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas; e Crimes digitais impróprios ou mistos (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc). são exemplos de crimes digitais impróprios os contra a honra praticados na internet, as condutas que envolvam trocas ou armazenamento de imagens com conteúdo

[8] NIGRI, D. F.. Crimes e segurança na internet. In Verbis, Rio de Janeiro: Instituto dos Magistrados do Brasil, Ano 4, n. 20, 2000.
[9] ROMEO CASABONA, Carlos Maria. De los delitos informáticos al cibercrimen: uma aproximación conceptual y político-criminal. El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales. Granada: Comares, 2006. P. 1.
[10] VIANNA, Tulio Lima. Fundamentos de direito penal informático. Rio de Janeiro: Forense, 2003.

> de pornografia infantil, o estelionato e até mesmo o homicídio."[11]

Deve se considerar que o processo de investigação relacionado a crimes praticados no âmbito da internet possui várias dificuldades em decorrência da prova digital, caracterizada por sua volatidade e instabilidade. [12]

A legislação brasileira, no que tange aos crimes digitais, ainda se encontra em crescimento, podendo se perceber que a legislação penal em alguns aspectos ainda não se encontra adequada no que tange a tutela jurídica relacionada a esses crimes. [13]

Um importante marco para o combate aos crimes cometidos na internet, foi a criação do Marco Civil da Internet, a Lei 12.965/14[14], procurando enfrentar temas ainda não tratados e não amparados por outras legislações. A lei tem como escopo proteger os registros, dados pessoais e comunicações privadas, neutralidade de rede e responsabilidade civil dos provedores de rede, a guarda de dados e registros e a requisição judicial de registros[15].

Entretanto, essa lei foi e ainda é muito criticada por peritos em informática e advogados de direito digital em aspectos como a tutela de registros de acesso e privacidade de usuários e liberdades de expressão.

Outro importante marco, foi a criação da Lei 12.737/12[16], a Lei Carolina Dieckmann, que ficou conhecida por esse nome após a invasão indevida de hackers à arquivos da atriz, onde foram divulgadas imagens em sites de pornografia, pelo fato de a vítima não ter aceitado a chantagem de pagar o dinheiro que os agentes estavam pedindo para não divulgarem suas imagens íntimas. O surgimento dessa norma, se mostrou importante na evolução do ordenamento jurídico brasileiro, considerando que trouxe um avanço em relação aos crimes cometidos em meios

---

[11] CRESPO, Marcelo. **Crimes Digitais.** Do que estamos falando? Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/

[12] MAGRIÇO, Manuel Eduardo Aires – A Exploração Sexual de Crianças no Ciberespaço – Aquisição e Valoração de Prova Forense de Natureza Digital, Sinapsis Editores, 2013, pág. 11.

[13] CRESPO, M. X. de F. Crimes Digitais. São Paulo: Saraiva, 2011.

[14] BRASIL, Marco Civil da Internet (2014). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

[15] TEFFÉ, C.S; MORAES, Maria Celina B. Redes Sociais Virtuais: privacidade e responsabilidade civil análise a partir do marco civil da internet. Pensar, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017.

[16] BRASIL, Lei Carolina Dieckmann (2012). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

digitais. [17] Essa lei, trouxe a tipificação do artigo 154-A do Código Penal[18], trazendo a conduta de invasão de dispositivo informático, recentemente esse artigo foi alterado pela Lei 14.155/21[19], que tornou mais rigorosa a pena de cometimento desse crime.

Apesar de ter havido a criação dessas Leis de regulamentação de crimes cometidos em meios virtuais, crimes como o de pornografia infantil virtual seguem aumentando, devendo haver outros novos mecanismos que abarquem essa nova variedade de crimes virtuais e suas peculiaridades.

3 DO CRIME DE PORNOGRAFIA INFANTIL

Para se entender sobre crimes sexuais, primeiramente cabe fazer uma análise das mudanças na legislação e na sociedade relacionada a esses crimes. A necessidade de se proteger os direitos fundamentais das crianças e adolescentes, ensejou a criação de declarações e convenções com esse intuito.

A demonstração expressa de preocupação com a pornografia infantil foi na Declaração Internacional dos Direitos das Crianças da Organização das Nações Unidas (ONU) realizada em Genebra em 1924, onde foi elencado os cinco princípios que devem assegurar as condições propícias para o desenvolvimento das crianças e adolescentes, como os princípios do desenvolvimento, da atenção, da ajuda, da formação e da educação.

No Brasil, após diversas discussões e conquistas internacionais acerca da temática, influenciadas pelas novas ideias da Convenção Internacional sobre o Direito da Criança, as organizações não governamentais começaram a lutar pela mudança na legislação brasileira, sendo que em 1988, com a Constituição Federal, houveram expressivas alterações, trazendo como dever da família, da sociedade e do Estado o zelo pela vida, saúde, alimentação, educação, lazer, cultura, profissionalização, dignidade, respeito, liberdade, convivência familiar e comunitária

[17] PAIXÃO, Gleice Kelly Silva. Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web. Goiânia, 2019

[18] BRASIL, Código Penal (1940). Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

[19] BRASIL, Lei 14.155 (2021). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm

todas as crianças, devendo que elas sejam resguardadas de qualquer tipo de negligência, discriminação, exploração, violência, crueldade e opressão, previsto no artigo 227 da Constituição Federal[20].

O artigo 227, §2º da Constituição Federal, também estabeleceu que a lei deve punir, de forma rigorosa, o abuso, a violência e a exploração sexual de criança e adolescente.

Logo após, em 1990 entrou em vigor o Estatuto da Criança e do Adolescente (ECA) previsto na Lei 8.069[21], sendo um importante marco para assegurar os direitos fundamentais desse grupo, tendo como objetivo a proteção das pessoas menores de idade devendo lhes ser assegurado o desenvolvimento físico, mental, moral, espiritual e social para que se possa alcanças a liberdade e dignidade das crianças e adolescentes. Esses direitos estão previstos no artigo 3º do ECA.

Com a adoção do artigo 227 na Constituição Federal, foi possível estabelecer o princípio da proteção integral da criança e do adolescente, previsto no artigo 1º do Estatuto da Criança e do Adolescente, devendo que o direito especializado seja dirigido a todos os jovens e a toda sua infância, não apenas a um grupo, devendo suas medidas de caráter geral serem aplicáveis para todos. [22]

Além do mais, o ECA prevê diversos crimes que podem ser cometidos contra a criança e o adolescente, esse artigo cuidará de se aprofundar mais especificamente no crime de pornografia infantil virtual.

O crime de pornografia infantil é classificado como crime digital impróprio pois já é tradicionalmente tipificado no ordenamento, sendo praticado com a ajuda da tecnologia. Assim, essa denominação representa os ilícitos penais tradicionais, que podem ser cometidos por meio de novo modo de atuar. [23]

No que tange a pornografia infantil, cabe trazer o entendimento de que é um equívoco denominar "pedofilia" os crimes de divulgação e armazenamento de

[20] BRASIL, Constituição Federal (1988). Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm
[21] BRASIL, Estatuto da Criança e do Adolescente (1990). Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm
[22] DA SILVA PEREIRA, Tânia. **Direito da criança e do adolescente: uma proposta interdisciplinar**. Renovar, 1996.
[23] Crespo, Marcelo Xavier de Freitas. Crimes digitais- São Paulo: Saraiva, 2011. P. 95

imagens com conteúdo de pornografia infantil, sendo também comum denominar a relação sexual de maiores com menores dessa forma. Porém, pedofilia é um transtorno de preferência sexual, uma parafilia, não havendo um crime com essa denominação no Brasil.[24]

A lei brasileira pune diversas infrações que envolvem a exposição da sexualidade infantil em fotos, imagens, filmagens e interpretações teatrais, como a produção, reprodução, filmagem e o registro de cenas de sexo explícito envolvendo crianças ou adolescentes. Sendo crime, também, transmitir, publicar, distribuir, adquirir, possuir e armazenar vídeos, fotografias e imagens envolvendo situações de pornografia com crianças e adolescentes. [25]

De acordo com o Estatuto da Criança e do Adolescente, é considerado criança, as pessoas com 12 anos incompletos, e adolescente, as com 12 anos completos até os 18 anos.[26] Essa previsão está no artigo 2º da referida Lei.

Os principais crimes que envolvem pornografia infantil estão elencados no Estatuto, em seus artigos 240 e seguintes. O Código Penal pune as condutas que envolvem relações sexuais com menores, como no caso de estupro de vulnerável, previsto no art. 217-A e outros, como de exploração da prostituição e tráfico de pessoas. [27]

Antes, o Estatuto da Criança e Adolescente previa apenas a divulgação e publicação, pela internet, de imagens e fotografias de crianças e adolescentes em atos pornográficos e cenas de sexo explícito, em seu artigo 241. Entretanto, a Lei 11.829/08[28], expandiu o núcleo do tipo penal, abrangendo entre outros, as condutas de armazenar, disponibilizar, expor à venda e transmitir imagens de abuso infantojuvenil, o artigo 240 passou a tratar da produção e o 241 da comercialização de material pornográfico infantil. [29]

[24] Crespo, Marcelo Xavier de Freitas. Crimes digitais- São Paulo: Saraiva, 2011. P. 99.
[25] Crespo, Marcelo Xavier de Freitas. Crimes digitais- São Paulo: Saraiva, 2011. P. 99
[26] Crespo, Marcelo Xavier de Freitas. Crimes digitais- São Paulo: Saraiva, 2011. P.99.
[27] Crespo, Marcelo Xavier de Freitas. Crimes digitais- São Paulo: Saraiva, 2011. P.99.
[28] BRASIL, Lei 11.829 (2008). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm
[29] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação: crimes cibernéticos.** 3 ed. rev. e ampl. – Brasília: MPF, 2016. P. 284

Dessa forma, o artigo 241-A, do ECA, traz a criminalização da publicação, troca ou divulgação de fotos ou vídeos contendo cena pornográfica ou de sexo explícito de criança ou adolescente, por qualquer meio de comunicação, inclusive nos meios digitais. Incorre no mesmo crime quem permitir meios para o armazenamento desses materiais em suas plataformas digitais. Porém, deve se ressaltar que os provedores de aplicativos de internet, só podem ser responsabilizados pelo crime se após uma notificação oficial feita pelo representante legal da criança ou adolescente, não cancelar o acesso ao conteúdo ilícito. [30]

Além do mais, o simples fato de se existirem imagens ou vídeos com esse conteúdo na internet, já é considerado crime, sendo irrelevante se o usuário teve ou não acesso ao conteúdo.

O ato de divulgar cenas de pornografia infantil, tem sua consumação no momento e ambiente que é permitido o acesso público na internet. Na denúncia é necessário que esteja descrita, a possibilidade de que aquele material esteja disponível em algum serviço de internet.

O crime previsto no artigo 241-B, trata da compra, posse ou guarda de material pornográfico envolvendo criança e adolescente, em algum dispositivo digital. Nesse caso, o agente detém apenas da posse do conteúdo, mas não o disponibiliza para outras pessoas, caso contrário estaria incorrendo no crime previsto no artigo 241-A do ECA. É possível que o agente que incorra nesse delito possa fazer jus da suspensão condicional do processo. [31]

Em todos os casos, é importante que seja feita uma perícia para a averiguação de se o agente não cometeu algum ato de abuso sexual também. Frisando que se o material que a pessoa possuir tiver ele próprio, incorrerá em provas de crime de estupro de vulnerável, previsto no artigo 217-A do Código Penal.

O artigo 241-C, trata da hipótese de montagem de imagem de criança ou adolescente que simule sua participação sem cena de sexo explícito ou pornografia, adulterando uma fotografia ou vídeo, incorrendo na mesma pena quem disponibilizar

[30] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação: crimes cibernéticos.** 3 ed. rev. e ampl. – Brasília: MPF, 2016. P. 284-287.
[31] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação: crimes cibernéticos.** 3 ed. rev. e ampl. – Brasília: MPF, 2016. P- 287-291.

esse conteúdo. O artigo 241-D trata da hipótese de convidar uma criança para relação libidinosa. E por fim, o artigo 241-E trata da disseminação de imagens que sejam a reprodução de cenas que envolvam a participação real de menores por meio de desenhos. [32]

Com essas considerações, pode se ter um conhecimento a respeito de como a legislação brasileira cuida da criminalização dos crimes cometidos contra a criança relacionados a delitos sexuais, cabendo no próximo tópico a exploração de como esse crime se aplica na prática e como seus índices são altos.

4 A PROBLEMÁTICA ACERCA DA PORNOGRAFIA INFANTIL VIRTUAL

Após o entendimento de o que são os crimes digitais e suas legislações e da legislação acerca da pornografia infantil, cabe fazer uma análise acerca desse assunto e como é importante o entendimento de como é sua atuação no Brasil, para que sejam encontradas soluções viáveis para enfrentar essa problemática.

O fato de a internet ser um lugar propício para que indivíduos possam se esconder atrás de uma identidade falsa, faz com que haja uma facilidade no contato com menores de idade tendo como objetivo a lascívia sexual. As vítimas, por sua inocência típica de sua idade e o seu desconhecimento dos riscos que podem existir ao utilizar a internet ou até mesmo por curiosidade, também muito típico nessa faixa etária, podem acabar por incorrerem em condutas lesivas, como à exploração sexual.

Os riscos de se utilizar a internet, podem ser, como estudado no tópico anterior, como a divulgação de imagens de menores de conteúdo sexual, a pornografia infantil e exposição do menor a esse tipo de conteúdo, além de diversos outros, como a oferta de serviços de prostituição, conversas de caráter sexual, intimidação, ameaça, *cyberbullyng*.

Assim como as crianças e adolescentes fazem uso da tecnologia com poucas informações sobre os riscos que a Internet pode ter, possuem na mesma medida poucos conhecimentos para prevenir esses riscos, não possuindo mecanismos de

[32] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação: crimes cibernéticos.** 3 ed. rev. e ampl. – Brasília: MPF, 2016. P. 291- 294.

como poderiam reagir diante de situações que lhe causarem medo, ou podem, também, não saber com quem falar em casos de necessidade. [33]

O aliciamento de crianças e adolescentes com o propósito sexual é a forma que os criminosos sexuais se utilizam de preparar suas vítimas para encontros sexuais. Além do mais, o agente pode usar da internet para esse intuito utilizando websites que reúnem características especificas das crianças.[34]

Vale ressaltar que para que possam conquistar a confiança das crianças e dos adolescentes os delinquentes podem se utilizam de perfis falsos e de uma linguagem acessível aos jovens, para que possam programar encontros virtuais e presenciais com o intuito de praticar atos de violência sexual, podem até oferecer oportunidades, como dinheiro, para que a vítima o encontre ou que mande fotos ou vídeos pornográficos. [35]

Um problema é o fato de que a divulgação da pornografia infantil na internet, torna muito complicada o processo de se identificar a origem do conteúdo, pois essa conduta delituosa se encontra mais presente em lugares como a Deep Web, local onde são encontrados materiais de difícil acesso presentes na internet, sendo esses matérias destinados a usuários específicos que acessam os conteúdos por links próprios, não estando presente facilmente nos sites convencionais na internet [36], sendo um local que torna muito complicada a identificação do agente que comete o crime, facilitando, por outro lado, a divulgação desse conteúdo por meio da internet e suas viabilidades. [37]

A Dark Web é uma rede onde ainda mais é utilizado o anonimato que surgiu pela disseminação da existência desse tipo de internet, que foi alcançando mais usuários com o passar dos anos. Essa internet é utilizada em governos que restringem o acesso a determinados sites, pois essa rede se utiliza da criptografia,

[33] BRETAN, M. E. A. N. Violência sexual contra crianças e adolescentes mediada pela tecnologia da informação e comunicação: elementos para a prevenção vitimal. 2012. Tese (Doutorado em Direito) -. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012.

[34] SANDERSON, Christiane. Abuso sexual em crianças: fortalecendo pais e professores pra proteger crianças contra abusos sexuais e pedofilia. São Paulo: M. Books, 2005.

[35] CASSANTI, Moisés de Oliveira. "Crimes virtuais, vítimas reais." *Rio de Janeiro: Brasport* (2014).

[36] SHIMABUKURO, A.; SILVA, M. G. B. de A. Internet, Deep Web e Dark Web. In SILVA, Ângelo Roberto Ilha da (Org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado. 2017.

[37] PAIXÃO, Gleice Kelly Silva. Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web. Goiânia, 2019

dificultando ainda mais o reconhecimento dos usuários e os possíveis crimes que possam vir a ocorrer. [38]

Dessa forma, por ambientes como esse é difícil o acesso e informação de o que está ocorrendo e por isso, a prática de crimes como a pornografia infantil é tão grande.

Para ter noção da abrangência que esse crime possui, cabe fazer a análise dos números e estatísticas. De acordo com dados divulgados na Safernet, as denúncias de pornografia infantil cresceram 33,45% em 2021 e os números seguem crescendo após o recorde histórico de denúncias que foram registradas em 2020. Em janeiro e abril de 2021 foram denunciadas à essa plataforma, 15.856 páginas relacionadas a esse crime e desse número, 7.248 foram removidas. [39]

No ano de 2020, a Safernet Brasil recebeu 98.244 denúncias anônimas de páginas de internet que continham pornografia infantil, tendo sido o maior número contabilizado desde que começou a ser feita a mediação, em 2006. No ano de 2019 foram registradas 48.576 páginas com esse conteúdo, tendo aumentado mais que o dobro o número em 102,24%. [40]

O presidente da Safernet afirma que esse fator pode ter sido caudado pelas mudanças que a pandemia causou na rotina das famílias, tendo as crianças ficado muito mais tempo nos meios digitais e consequentemente mais expostas a situações de risco, tendo piorado como o fechamento das escolas que costuma contar com uma rede de apoio para a prevenção de violência sexual. [41]

Dados colhidos na Ouvidoria Nacional de Direitos Humanos (ONDH), em 2020, mostraram que o Disque 100, utilizado para fazer denúncias de abuso e

[38] SHIMABUKURO, A.; SILVA, M. G. B. de A. Internet, Deep Web e Dark Web. In SILVA, Ângelo Roberto Ilha da (Org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado. 2017.

[39] Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta Safernet Brasil. **Safernet**, 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil#mobile

[40] Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta Safernet Brasil. **Safernet**, 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil#mobile

[41] Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta Safernet Brasil. **Safernet**, 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil#mobile

exploração sexual de crianças e adolescentes, registrou 23.351 denúncias de violação sexual, havendo um aumento de 23, 4% relacionado ao ano de 2019. [42]

Nos 15 anos de funcionamento da Safernet, foram recebidas e processadas 1.759.354 denúncias anônimas de pornografia infantil, sendo 429.665 páginas diferentes e desse total, 340.005 foram removidas da internet por conterem indícios de crimes. [43]

Com esses dados pode se perceber a incidência altíssima desse crime nos meios digitais. Considerando que esses números se referem apenas ao conteúdo que foi achado e denunciados, o número é mais alto ainda considerando o conteúdo que não foi encontrado e denunciado.

De acordo com um estudo realizado em outubro de 2012 pelo CGI (Comitê Gestor da Internet), 2,70% de jovens entre 9 e 16 anos possuem seu próprio perfil em algum site de relacionamento e desses 13% postam o endereço de suas casas e divulgam seus telefones. Foi apontado também que as crianças não tem receio em publicar informações privadas, sendo que 86% possuem uma foto de seu rosto publicada, 69% já divulgaram seu sobrenome e 28% informaram onde estudam. 23% já tiveram contato com desconhecidos ou já tiveram encontros reais. [44]

Ademais um outro estudo da Internet Watch Foundation (IWF) comprovou que 88% das imagens e vídeos de conteúdo erótico ou sexual produzidos pelos próprios jovens, foram publicados em redes sociais ou sites com emissões de webcam, tendo sido captadas e republicadas em outros sites, sem permissão. [45]

Dessa forma, pode se entender que essa conduta de ter imagens e vídeos eróticos distribuídos sem controle na internet podem trazer sérios danos à criança, podendo ser humilhada e molestada, passando a sofrer com diversos problemas como ansiedade, depressão, isolamento social, entre outros.

[42] Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta Safernet Brasil. **Safernet**, 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil#mobile

[43] Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta Safernet Brasil. **Safernet**, 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil#mobile

[44] CASSANTI, Moisés de Oliveira. "Crimes virtuais, vítimas reais." *Rio de Janeiro: Brasport* (2014).

[45] CASSANTI, Moisés de Oliveira. "Crimes virtuais, vítimas reais." *Rio de Janeiro: Brasport* (2014).

Uma das melhores formas de se combater a pornografia infantil é por meio de denúncias para que assim os órgãos competentes possam excluir esse conteúdo da internet e é necessário um apoio e proteção a criança e adolescente, dentre essa rede pode ser citado os Conselhos Tutelares, as Varas da Infância e Juventude, Delegacias de Proteção à Criança e Adolescente, entre outros.

A Lei 13.441/17[46], trouxe uma inovação para o Estatuto da Criança e do Adolescente, acrescentando os artigos 190-A ao 190-E, trazendo a possibilidade de infiltração de Agentes de Polícia para a Investigação de Crimes contra a dignidade sexual de criança e de adolescente, tornando-se uma conduta lícita.

Com essa inovação, o instituto policial possui instrumentos que os mantém anônimos nas redes e possam rastrear as possíveis irregularidades que os criminosos cometem em ambientes como a Deep web e Dark Web. [47]

Além do mais, nos delitos de disseminação de pornografia infantil via web, é possível que nas investigações feitas em um país, sejam identificados IP'S e dados utilizados para conexão que serviram de apoio na prática criminosa de usuários de Internet que estão em outro país. Dessa forma, a polícia desse país envia as informações de onde os IP's foram localizados para que haja a investigação das possíveis provas de atos ilícitos a partir desse local. Nos casos envolvendo esse tipo de troca de informação entre países, pode ocorrer por intermédio da INTERPOL.[48]

É muito importante que além de outras medidas na legislação como as mencionadas e nos ambientes virtuais, os pais procurem ter conhecimento sobre o tipo de conteúdo que os filhos estão consumindo na internet e expliquem sobre seus riscos também, mantendo sempre um diálogo a respeito dessas situações, para que as crianças não sejam ludibriadas e enganadas na internet.

[46] BRASIL, Lei 13.441 (2017). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13441.htm

[47] PAIXÃO, Gleice Kelly Silva. Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web. Goiânia- GO, 2019

[48] POLÍCIA FEDERAL. Combate a disseminação de pornografia infantil pela deep web no Rio Grande do Sul. 15 de outubro de 2014.

5 CONSIDERAÇÕES FINAIS

O artigo teve como intenção discutir a problemática acerca da pornografia infantil, que com o avanço da internet e das novas tecnologias e plataformas digitais, teve um aumento em seu número e propagação.

Para entender o problema de forma abrangente, foi estudado o contexto acerca dos crimes cometidos nos meios digitais e as facilidades que os delinquentes tem de cometerem atos ilícitos por esses meios, entendendo como foi importante a criação de mecanismos e legislações que pudessem criminalizar essas condutas e tirar o conceito enraizado na cabeça da sociedade de que a internet seria uma "terra sem leis".

Foi estudado também o avanço ao longo do tempo que das legislações acerca da criança e do adolescente e como esse avanço foi de extrema importância para proteger os direitos fundamentais desse grupo e como mesmo assim, ainda deve haver outros tipos de mecanismos para combater os crimes cometidos contra as crianças e adolescentes.

Foi observado, também, como os jovens são vulneráveis no meio da internet por não entenderem e não possuírem conhecimentos suficientes para que possam enxergar possíveis ameaças em meios digitais, por isso é muito importante que cada vez mais esse grupo seja conscientizado acerca dos riscos.

Além do mais, a pornografia infantil virtual é um grande problema na sociedade atual o que pode trazer muitos danos, tanto para as crianças que tem acesso a esse tipo de conteúdo, quanto para as crianças que sofrem e estão presentes no crime. Cada vez mais, as legislações tem procurado maneiras de acabar com esse crime, mas ainda se encontra muito longe de ter o sucesso efetivo, devendo haver um trabalho da sociedade com o Estado e Poder judiciário para poder haver uma efetiva redução desse crime.

REFERÊNCIAS

BRASIL, **Constituição Federal (1988)**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL, Estatuto da Criança e do Adolescente (1990). Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm

BRASIL, **Lei Carolina Dieckmann (2012).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

BRASIL, **Código Penal (1940).** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

BRASIL, **Lei 11.829 (2008).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm

BRASIL, **Lei 13.441 (2017).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13441.htm

BRASIL, **Lei 14.155 (2021).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm

BRASIL, **Marco Civil da Internet** (2014). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação: crimes cibernéticos.** 3 ed. rev. e ampl. – Brasília: MPF, 2016. P- 287-291.

BRETAN, M. E. A. N. **Violência sexual contra crianças e adolescentes mediada pela tecnologia da informação e comunicação: elementos para a prevenção vítima**. 2012. Tese (Doutorado em Direito) -. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012.

CASSANTI, Moisés de Oliveira**. "Crimes virtuais, vítimas reais."** *Rio de Janeiro: Brasport* (2014).

CRESPO, Marcelo Xavier de Freitas**. Crimes digitais**- São Paulo: Saraiva, 2011. P.99.

CRESPO, Marcelo. **Crimes Digitais.** Do que estamos falando? Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/

DA SILVA PEREIRA, Tânia. **Direito da criança e do adolescente: uma proposta interdisciplinar**. Renovar, 1996.

MAGRIÇO, Manuel Eduardo Aires – **A Exploração Sexual de Crianças no Ciberespaço – Aquisição e Valoração de Prova Forense de Natureza Digital**, Sinapsis Editores, 2013, pág. 11.

NIGRI, D. F. **Crimes e segurança na internet**. In Verbis, Rio de Janeiro: Instituto dos Magistrados do Brasil, Ano 4, n. 20, 2000.

PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia, 2019

POLÍCIA FEDERAL. **Combate a disseminação de pornografia infantil pela deep web no Rio Grande do Sul**. 15 de outubro de 2014.

ROMEO CASABONA, Carlos Maria. **De los delitos informáticos al cibercrimen**: uma aproximación conceptual y político-criminal. El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales. Granada: Comares, 2006. P. 1.

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

SAFERNET. 2021.Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta Safernet Brasil. **Safernet**, 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil#mobile

SANDERSON, Christiane. **Abuso sexual em crianças**: fortalecendo pais e professores pra proteger crianças contra abusos sexuais e pedofilia. São Paulo: M. Books, 2005.

SERRA, Thalyta Maia Galvão. **A pedofilia na internet à luz do estatuto da criança e do adolescente**. 2009. 86 f. Monografia (Graduação em direito) – FESP Faculdades, João Pessoa. 2009.

SHIMABUKURO, A.; SILVA, M. G. B. de A. **Internet, Deep Web e Dark Web**. In SILVA, Ângelo Roberto Ilha da (Org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado. 2017.

TEFFÉ, C.S; MORAES, Maria Celina B. **Redes Sociais Virtuais: privacidade e responsabilidade civil análise a partir do marco civil da internet**. Pensar, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017.

VIANNA, Tulio Lima**. Fundamentos de direito penal informático**. Rio de Janeiro: Forense, 2003.

DESIGUALDADE DE GÊNERO NA INTERNET E OS PARÂMETROS REGULATÓRIOS NO COMBATE À VIOLÊNCIA CONTRA MULHER

Natália Rocha Damasceno[1]

RESUMO

O presente trabalho tem como objeto abarcar os parâmetros de regulação na internet sob o foco no combate à violência de gênero. Procura-se estabelecer quais são as leis especializadas e voltadas ao mundo online que visam proteger a mulher no âmbito criminal, bem como no âmbito cível e no âmbito particular. A proposta é entender quais temas estão devidamente protegidos por tais parâmetros regulatórios e quais são essas leis, bem como o contexto que se inserem e sua aplicação. No âmbito criminal, analisa-se a Lei nº 12.737/2012; Lei nº 13.718/2018; Lei nº 13.772/2012; e Lei nº 13.642/18. No âmbito cível, se examina o Marco Civil da Internet e, no âmbito particular, estabelece-se os parâmetros para retirada de conteúdo nos Termos de Uso do Instagram Twitter e Facebook.

Palavras-chave: desigualdade de gênero; regulação da internet; crimes cibernéticos.

ABSTRACT

The present work aims to cover the parameters of regulation on the internet with a focus on combating gender violence. It seeks to establish which are the specialized laws geared to the online world that aim to protect women in the criminal sphere, as well as in the civil and private spheres. The proposal is to understand which themes are duly protected by such regulatory parameters and which are these laws, as well as the context and their application. In the criminal sphere, Law No. 12,737 / 2012 is analyzed; Law No. 13,718 / 2018; Law No. 13,772 / 2012; and Law No. 13.642/ 2018. In the civil scope, the Marco Civil da Internet is examined and, in the private scope, the parameters for withdrawing content are established in the Instagram Twitter and Facebook Terms of Use.

Key words: gender inequality; regulation of the internet; cybercrimes.

[1] Pós-graduanda em Direito Digital pelo UniCeub. Graduada em Direito pelo UniCeub. E-mail: nataliardamascenogmail.com. Artigo elaborado como requisito parcial para aprovação na matéria Crimes Digitais, ministrada pelo Professor Paulo Binicheski.

1 INTRODUÇÃO

O presente trabalho tem como objeto abarcar os parâmetros de regulação na internet sob o foco no combate à violência de gênero. Procura-se estabelecer quais são as leis especializadas e voltadas ao mundo online que visam proteger a mulher no âmbito criminal, bem como no âmbito cível e no âmbito particular. A proposta é entender quais temas estão devidamente protegidos por tais parâmetros regulatórios e quais são essas leis.

A importância do tema se dá pela manutenção da desigualdade de gênero durante anos e que, com o advento da internet, se adaptou ao "mundo virtual". Verifica-se que é necessário a ação afirmativa do Estado e da sociedade para a proteção da mulher, na tentativa de trazer efetividade à igualdade constitucional trazida pelo art. 5º, I, CF.

Neste sentido, o primeiro capítulo busca demonstrar a amplitude global que a internet possui. Afere-se que, apesar de muitos efeitos positivos e de uma verdadeira ressignificação das relações sociais, a internet também é um espaço em que se reproduz desigualdades sociais e muita violência. O segundo capítulo trata sobre os dispositivos normativos criminais e especializados para a proteção da mulher no mundo virtual, percebendo-se que as leis até agora elaboradas tiveram forte influência de casos reais de violência de gênero na internet.

No terceiro capítulo aborda-se as possibilidades de retirada de conteúdo da internet, a partir de uma análise do Marco Civil da Internet sobre, principalmente, o instituto da responsabilidade civil dos provedores de internet, e da retirada de conteúdo das redes. No quarto capítulo é analisada a retirada de conteúdo determinada pelo próprio provedor de internet, a partir do exame dos Termos de Uso do Twitter, Instagram e Facebook. Neste capítulo, afere-se que as redes sociais não são tão transparentes quanto às informações de retirada de conteúdo.

2 ALCANCE E CONSEQUÊNCIAS DA INTERNET NA SOCIEDADE

2.1 Amplitude global da internet e seus efeitos

O Brasil teve seu primeiro contato com a internet em 1988, quando a Fundação de Amparo à Pesquisa do Estado de São Paulo se conectou com um centro de pesquisa científica dos Estados Unidos[2]. Naquele mesmo ano, era promulgada a Constituição da República, que já cuidava de garantir normativamente o tratamento prioritário à pesquisa cientifica básica e tecnológica. Além disso, a Carta assegurou incentivo ao desenvolvimento científico, à pesquisa e à capacitação tecnológica (art. 218, redação original). Mais tarde, com o avento da EC n. 85 de 2015, garantiu-se também a inovação.

Em 2020, são mais de 4.8 bilhões de usuários da internet em todo o mundo[3]. No Brasil, isso corresponde 76% da população, alcançando um número de 158,46 milhões de pessoas em 2018[4]. E pode-se visualizar os efeitos desses números significativos na prática. As pessoas se expressam por meio das redes sociais, se informam pelos noticiários online, pesquisam por mecanismos de busca, fazem cursos educacionais por meio de plataformas voltadas ao ensino, debatem nos comentários de postagens, leem e-books, organizam agendas, fazem reuniões, compram produtos e muito mais.

A importância da internet é nítida. Essa tecnologia trouxe aspectos positivos relevantes para a sociedade, tornando tudo – à primeira vista – mais fácil e acessível. A informação se tornou democrática, a comunicação agora é simples, pode-se pedir comida num minuto e, no outro, se inscrever numa vaga de emprego. A internet está tão intrínseca na vida moderna que quase já não dá mais para se utilizar da dicotomia

[2] VIEIRA, Eduardo. **Os bastidores da internet**: a história de quem criou os primeiros negócios digitais no Brasil. 2003.

[3] Precisamente, são 4.833.521.806 (quatro bilhões e oitocentos e trinta e três milhões e quinhentos e vinte e um mil e oitocentos e seis) usuários em 30 de junho de 2020. Disponível em <https://www.internetworldstats.com>. Acesso em: 28 de set. 2020.

[4] CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros - TIC Domicílios 2017. Inclui os usuários de Internet, os usuários de Internet no telefone celular e os usuários de aplicações que necessitam de conexão à Internet.

"real" e "virtual". As duas perspectivas se confundem e ao que parece se tornaram inseparáveis.

Entretanto, assim como o mundo "real" e, principalmente, com a popularização das redes sociais, a internet também se tornou uma ferramenta perigosa. Se configurando como um lugar de expressão da sociedade, manuseada por indivíduos pertencentes a singularidades, opressões, vivências, preconceitos e tudo o que há num ser-humano, o uso da internet que antes só era visto como solução agora também faz parte do problema. E que problema! São *fake news*, vírus, spams, *bots*, golpes cibernéticos, *deepfakes*, falta de privacidade, *cookies*, algoritmos manipulados e outros. Ainda que muitas dessas ferramentas sejam tidas como novas, elas também contribuem para fortalecer velhos conhecidos. É o caso da desigualdade de gênero.

2.2 Desigualdade de gênero e iniciativas de proteção à mulher

O primeiro dos setenta e oito incisos que dispõem sobre os direitos sociais fundamentais do art. 5º da Carta Magna assegura que homens e mulheres são iguais em direitos e obrigações, nos termos da Constituição. Nada obstante, a desigualdade de gênero pode ser reparada em cada canto das relações humanas.

No âmbito político, por exemplo, o direito ao voto feminino só foi equiparado ao do homem com o Código Eleitoral de 1965, quando passou a ser obrigatório para homens e mulheres em todo o país[5]. Ainda hoje, há reflexos dessa resistência: nas eleições de 2018, haviam apenas 31,12% candidatas para o cargo de deputada estadual/distrital, e 31,64% disputavam para deputada federal[6];– foram eleitas 77

[5]LIMONGI, Fernando; OLIVEIRA, Juliana de Souza; SCHMITT, Stefanie Tomé. Sufrágio universal, mas... só para homens. O voto feminino no Brasil. Revista de Sociologia e Política v. 27, n. 70, 2019, p. 18. Disponível em <https://www.scielo.br/pdf/rsocp/v27n70/0104-4478-rsocp-27-70-e003.pdf>. Acesso em: 3 de jun. 2020.

[6] BACKES, Ana Luiza *et al.* Breve Análise dos Dados sobre candidaturas de Mulheres nas Eleições de 2018. Estudo técnico. 2019. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/comissao-de-defesa-dos-direitos-da-mulher-cmulher/arquivos-de-audio-e-video/breve-analise-dos-dados-sobre-candidatas-eleitas-receitas-nas-eleicoes-de-2018> Acesso em: 7 de mar. 2020.

mulheres no total de 513 de deputados, e somente 12 senadoras dentre os 81, ocupando 15% do Parlamento[7].

Nas relações de trabalho, uma pesquisa do IBGE realizada em 2018 demonstrou que mulheres brancas ganham 79.5% do total do salário pago ao homem branco, e que mulheres negras ganham 80,1% do salário do homem negro. As ocupações das mulheres são principalmente relacionadas ao cuidado, trabalhos domésticos ou ensino primário – características próprias do estereótipo de gênero. 95% trabalhadores de serviços domésticos e 84% professores de ensino fundamental são mulheres. Quando se fala em espaços de poder, apenas 41,8% são diretoras e gerentes, ganhando 71,3% do salário dos homens[8].

No âmbito de segurança pública, as mulheres e meninas também são atingidas apenas por sua condição de gênero. Em 2019, foram 1.206 vítimas de feminicídio, onde o ápice da mortalidade se deu aos 30 anos, havendo 61% mulheres negras e 70,7% possuíam apenas o ensino fundamental; 88,8% do homicídio qualificado foi cometido por companheiro ou ex-companheiro. Sobre violência sexual, os dados informam que para cada dois minutos há um registro de assédio; são 180 estupros por dia e, dessas, 4 meninas até 13 anos estupradas por hora[9]. Apesar dos números alarmantes, sabe-se que os dados supracitados são apenas exemplos. Deve ser considerada a subnotificação e as nuances de classe e raça que afetam e invisibilizam as mulheres pretas.

Como visto, apesar da igualdade formal entre homens e mulheres, percebe-se que a equidade material está longe de ser alcançada. Assim, sendo o coletivo de mulheres um grupo socialmente oprimido, cabe ao Estado promover políticas afirmativas para efetivar os direitos e garantias constitucionais voltadas para a igualdade de gênero. A Lei Maria da Penha (Lei nº 11.340/2006); o feminicídio como qualificadora do crime de homicídio (Lei n. 13.104/2015); e a Lei da

[7] No Senado, foram eleitos 47 homens e apenas 7 mulheres. Na Câmara, 436 homens e 77 mulheres. Nas Assembleias, 898 homens foram eleitos e apenas 161 mulheres. (TSE. Número de mulheres eleitas em 2018 cresce 52,6% em relação a 2014. Disponível em <http://www.tse.jus.br/imprensa/noticias-tse/2019/Marco/numero-de-mulheres-eleitas-em-2018-cresce-52-6-em-relacao-a-2014> Acesso em: 3 de jun. 2020).

[8] IBGE. Diferença do rendimento do trabalho de mulheres e homens nos grupos ocupacionais - Pnad Contínua 2018, que o Instituto Brasileiro de Geografia e Estatística (IBGE).

[9] Anuário Brasileiro de Segurança Pública. 2019. p. 7.

Importunação Sexual (13.718/2018), foram algumas das ações do Poder Legislativo que contribuíram para a proteção da mulher.

A Suprema Corte, enquanto guardiã da Constituição, também colaborou para o enfrentamento das desigualdades de gênero: descriminalizou o aborto de feto anencéfalo (ADPF 54); reputou inconstitucional edital de concurso que previa apenas participantes apenas do sexo masculino em prova de policial militar (RE 528.684); declarou a inconstitucionalidade da diferenciação entre períodos da licença-maternidade biológica e adotiva (RE 778889); e consignou a obrigatoriedade de se aplicar o mínimo de 30% do fundo partidário para a campanha de mulheres (ADI 5617). São apenas alguns exemplos.

Entretanto, percebe-se que, mesmo com algumas ações afirmativas que buscam dar efetividade aos direitos das mulheres, a estrutura desigual da sociedade se sustenta. Isso porque a relação de superioridade que o homem tem sobre a mulher é reproduzida todos os dias e em todos os âmbitos: domésticos, públicos, sociais e privados. Em breves palavras, construiu-se, durante séculos, uma espécie de "senso comum" em que à mulher caberia apenas os afazeres domésticos, o cuidado dos filhos e a subordinação ao homem. O masculino, por sua vez, estaria livre das responsabilidades da vida familiar para dedicar-se à vida "pública", onde decisões importantes são tomadas[10].

Esses estereótipos são reproduzidos constantemente em todos os ciclos sociais, e o usuário de internet passou a ganhar destaque no papel de sua manutenção. Como uma verdadeira extensão do mundo real, percebeu-se que o espaço *online* se tornou palco para muitas violências de gênero. Essas violências, entretanto, nem sempre vêm da mesma forma, ou na mesma "intensidade". Podem ser ataques diretos à condição da mulher, como divulgação de fotos íntimas sem autorização, ou podem surgir de forma mais implícita, como comentários que atacam a vida pessoal da mulher, seu corpo, suas escolhas íntimas. Abaixo, analisa-se melhor essas diferenciações de violências.

[10] BIROLI, Flávia. Divisão Sexual do Trabalho e Democracia. DADOS – Revista de Ciências Sociais, Rio de Janeiro, vol. 59, no 3, 2016. p. 726-727. Disponível em <http://www.scielo.br/pdf/dados/v59n3/0011-5258-dados-59-3-0719.pdf>.Acesso em: 12 de mar. 2020.

Algumas dessas violências podem ser percebidas facilmente, ao passo que são crimes, ataques diretos e explícitos. No ponto, pode-se citar alguns casos recentes como exemplo. Em setembro de 2020, descobriu-se que o facebook foi utilizado como ferramenta para um grupo que incentiva a necrofilia, onde seus integrantes postam fotos de mulheres e meninas mortas (como vítimas de acidentes) conjuntamente com frases como "festa no IML", normalizando a conjunção carnal com mulheres mortas[11]. Em outra página descoberta em junho de 2020, homens se sentem à vontade para compartilhar fotos de roupas íntimas de meninas e mulheres, muitas sendo suas filhas, enteadas, esposas ou sobrinhas, acabando por contribuir com a pedofilia e incentivando o abuso sexual[12].

Outras violências não são tão explícitas assim, sendo mais ocultas. Essas são justificadas por serem "opiniões", por ser um exercício da "liberdade de expressão", mas, na verdade, carregam características misóginas que influenciam a desigualdade de gênero. Como exemplo, um comentário numa comunidade do Reddit: "Posso entender as mulheres que pretendem saber o que é um bom homem. Claro, é um sujeito de que podem se aproveitar. Mas o que as leva a crer que podem definir o que é um homem de verdade? Se você tem vagina, não tem nem ideia do que é um homem. Os homens, por outro lado, sabem exatamente o que é uma mulher de verdade. Só têm que recordar como eles eram aos 12 anos. As mulheres não amadureceram moralmente depois da puberdade"[13]

Portanto, percebe-se que, a depender de quem está atrás de um dispositivo com acesso à rede, a internet pode virar uma forte ferramenta de manutenção da desigualdade de gênero, em diversas formas e em vários níveis de intensidade. Focando no âmbito online, portanto, percebe-se que, como resposta, há diversas leis específicas visando coibir as violências acima explicitadas.

---

[11] FOLHA. Grupos em redes sociais incentivam necrofilia. Disponível em <https://www1.folha.uol.com.br/cotidiano/2020/09/grupos-em-redes-sociais-incentivam-necrofilia.shtml>. Acesso em 1 de out. 2020.

[12] PLANTÃO190. Mulheres denunciam grupo repugnante. Disponível em <https://plantao190.com.br/mulheres-denunciam-grupo-repugnante-e-as-conversas-sao-de-embrulhar-o-estomago/>. Acesso em 1 de out. De 2020.

[13] EL PAÍS. A incontrolável ascensão dos ninhos de machismo na Internet. Disponível em <https://brasil.elpais.com/sociedade/2020-02-07/incels-machos-atras-de-mulher-a-incontrolavel-ascensao-dos-ninhos-de-machismo-na-internet.html>. Acesso em: 1 dez. 2020.

Assim, os próximos capítulos destinam-se a analisar os principais parâmetros de normativos específicos da internet contra a desigualdade de gênero no âmbito criminal, cível e particular.

3 OS PARÂMETROS DE REGULAÇÃO NO ÂMBITO CRIMINAL

3.1 Lei nº 12.737/2012 (Lei Carolina Dieckmann)

A Lei de nº 12.737 de 30 de novembro de 2020 incluiu e alterou dispositivos ao Código Penal para tipificar criminalmente os delitos informáticos (154-A, 154-B, 266 e 268, CP)[14]. Esse normativo foi a primeira lei especial no Brasil que cuidou de tratar, especificamente, dos crimes cibernéticos. Antes da promulgação da referida lei, havia uma lacuna no ordenamento jurídico, que obrigava os magistrados a se utilizarem da analogia para coibirem ações ilícitas no meio online.[15]

A tramitação de seu Projeto de Lei nº 2.793/11 ganhou celeridade quando a atriz brasileira Caroline Dieckmann foi vítima de violência de gênero na internet, momento em que 36 fotos íntimas foram divulgadas por um *hacker*. O caso gerou grande repercussão no Brasil, chegando a ser um dos assuntos mais comentados do país e do mundo. A sociedade, então, pressionou por respostas do Poder Legislativo, o que ocasionou na aprovação do PL em 30 de novembro de 2012.

Em síntese, o art. 154-A e o art. 154-B insere o tipo penal de "invasão de dispositivo informático" para obter, adulterar ou destruir dados ou informações sem autorização do titular, aumentando a pena a até dois terços de houver divulgação de informações sigilosas. No art. 154-B se designa que, em regra, o processo será por meio de uma ação penal pública condicionada a representação. Além disso, no art. 266, §1º, CP, estabelece a pena de detenção de um a três anos e multa a quem interrompe serviço telemático ou de informação de utilidade público, impedindo ou dificultando o restabelecimento. O §2º do mesmo dispositivo afirma que a pena será em dobro se o crime é cometido em calamidade pública. Ainda, o parágrafo único do

[14] PLANALTO. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 1 dez. 2020.

[15] REIS, Wanderlei José dos. DELITOS CIBERNÉTICOS: IMPLICAÇÕES DA LEI Nº 12.737/12. RIDB, Ano 3 (2014), nº 8. Disponível em <https://www.cidp.pt/revistas/ridb/2014/08/2014_08_05983_05994.pdf>. Acesso em: 1 dez. 2020.

art. 298 equipara o cartão de crédito/débito a documento particular para crime de falsificação.

Algumas fragilidades foram fortemente apontadas pela doutrina: as penas ínfimas a quem comete o crime; a inocorrência de delito a quem tenha "apenas" espionado os dados; a utilização do termo "invasão", pois necessitaria de um mecanismo de segurança para ser corrompido; e, além disso, pelo fato de que a lei específica veio antes de uma "regra geral", ou seja, antes da aprovação do Marco Civil da Internet.[16]

3.2 Lei nº 13.718/2018 e Lei nº 13.772/2012: combate contra o *'revenge porn'*

O termo *"revenge porn",* ou pornografia de vingança – em tradução literal, veio à tona para, inicialmente, definir os casos em que um ex-companheiro divulga conteúdo íntimo de teor sexual na internet. Entretanto, percebeu-se que não obrigatoriamente essa prática necessite ter uma motivação para a dita 'vingança', ou um conteúdo pornográfico, por isso, utiliza-se hoje a expressão "disseminação não consentida de imagens íntimas" [17]. O ilícito ganhou visibilidade da mídia e da sociedade em geral quando, em 2013, duas meninas se suicidaram após serem vítimas desse ataque[18].

No que tange à Lei nº 13.718/2018, foi criado o tipo penal do art. 218-C, CP, que considera crime a divulgação de cena de estupro, cena de sexo ou pornografia, com pena aumentada se o crime é praticado por quem tenha relação íntima com a vítima[19]:

[16] OLIVEIRA, Claudio Roberto de Almeida. A extimidade da sociedade digital e a eficácia da Lei 12.737/12 - invasão de dispositivo informático. Disponível em <http://www.conteudojuridico.com.br/consulta/Artigos/44141/a-extimidade-da-sociedade-digital-e-a-eficacia-da-lei-12-737-12-invasao-de-dispositivo-informatico>. Acesso em: 1 dez. 2020.

[17] NERIS, Natália; RUIZ, Juliana Pacetta; VALENTE, Mariana Giorgetti. Análise comparada de estratégias de enfrentamento a "revenge porn" pelo mundo. doi: 10.5102/rbpp.v7i3.4940. Disponível em <https://www.publicacoes.uniceub.br/RBPP/article/download/4940/3656> Acesso em: 1 dez. 2020. p. 335-336.

[18] FORUM. Pornografia de revanche: em dez dias, duas jovens se suicidam. Disponivel em <https://revistaforum.com.br/noticias/revenge-porn-divulgacao-de-fotos-intimas-culmina-com-suicidio-de-duas-jovens/>. Acesso em: 1 dez. 2020.

[19] PLANALTO. LEI Nº 13.718, DE 24 DE SET. DE 2018. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm>. Acesso em: 1 dez. 2020.

> "Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia
>
> Art. 218-C. 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:
>
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.
>
> Aumento de pena
>
> § 1º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação.
>
> Exclusão de ilicitude
>
> § 2º Não há crime quando o agente pratica as condutas descritas no caput deste artigo em publicação de natureza jornalística, científica, cultural ou acadêmica com a adoção de recurso que impossibilite a identificação da vítima, ressalvada sua prévia autorização, caso seja maior de 18 (dezoito) anos."

A Lei nº 13.772/2012, por sua vez, altera a Lei Maria da Penha e o Código Penal, "para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado"[20]. Assim, no art. 7º da Lei 11.340/06, passa-se a considerar formas de violência doméstica e familiar contra as mulheres:

> II - a violência psicológica, entendida como qualquer conduta que lhe cause dano emocional e diminuição da autoestima ou que lhe prejudique e perturbe o pleno desenvolvimento ou que vise degradar ou controlar suas ações, comportamentos, crenças e decisões, mediante ameaça, constrangimento, humilhação, manipulação, isolamento, vigilância constante, perseguição contumaz, insulto, chantagem, violação de sua intimidade, ridicularização, exploração e limitação do direito de ir e vir ou qualquer outro meio que lhe cause prejuízo à saúde psicológica e à autodeterminação;

Já no Código Penal, houve a inclusão do art. 216-B, para tipificar o crime de registro não autorizado da intimidade sexual:

[20] PLANALTO. LEI Nº 13.772, DE 19 DE DEZEMBRO DE 2018. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13772.htm>. Acesso em: 1 dez. 2020.

> Art. 216-B. Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes:
>
> Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa.
>
> Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo."

3.3 Lei nº 13.642 de 3 de abril de 2018 (Lei Lola)

A Lei nº 13.642 de 3 de abril de 2018, chamada Lei Lola, também contém em sua tramitação a violência virtual contra mulher. A Dolores (Lola) Aronovich, autora de um blog feminista, chamado "Escreva Lola Escreva", que publica e se dedica a expor as manifestações de ódio contra mulheres na rede. A Lei apelidada por seu nome acrescenta a competência para a Polícia Federal "no que concerne à investigação de crimes praticados por meio da rede mundial de computadores que difundam conteúdo misógino, definidos como aqueles que propagam o ódio ou a aversão às mulheres.".

Dessa forma, inclui ao art. 1º da Lei nº 10.446/02 o inciso VII, que dispõe:

> Art. 1º Na forma do inciso I do § 1º do art. 144 da Constituição, quando houver repercussão interestadual ou internacional que exija repressão uniforme, poderá o Departamento de Polícia Federal do Ministério da Justiça, sem prejuízo da responsabilidade dos órgãos de segurança pública arrolados no art. 144 da Constituição Federal, em especial das Polícias Militares e Civis dos Estados, proceder à investigação, dentre outras, das seguintes infrações penais:
>
> **VII – quaisquer crimes praticados por meio da rede mundial de computadores que difundam conteúdo misógino, definidos como aqueles que propagam o ódio ou a aversão às mulheres**.

Em seu blog, a autora que leva o apelido da Lei conta a importância da disposição normativa e como isso contribuiu para sua trajetória:

> A lei é muito importante porque, como o meu caso (e de tantas outras mulheres) mostra, quem nos ataca pela internet raramente é punido. Eu sou ameaçada de morte e atacada pelo menos desde 2011 por misóginos assumidos. Já fiz onze boletins de ocorrência, tem inquérito aberto, a PF investiga desde dezembro do ano passado (quando o reitor da UFC, universidade onde trabalho, recebeu um email dizendo que, se

> eu não fosse exonerada, ele passaria uma semana recolhendo pedaços de 300 cadáveres). Mas investiga por crime de terrorismo, não pelas milhares (literalmente) de ameaças que recebi e ainda recebo.
>
> Tenho um e-mail de um superintendente da PF, de 2015, dizendo que eles não iriam investigar os ataques a mim, porque eles só atuam nas áreas em que o Brasil é signatário internacional (racismo e pornografia infantil -- crimes cometidos às dúzias pela quadrilha que me persegue). (...) Por incrível que pareça, um dos próprios criadores do site me denunciou ao Ministério Público, que acatou a denúncia contra mim! Fui chamada para depor na PF e "provar" que o site não era meu (felizmente, eu havia feito um BO um mês antes). Mas o nível do absurdo era surreal. Não só a PF não ajudou (e declarou que não iria ajudar) a ir atrás dos culpados, que eu e toda a torcida do Flamengo sabemos quem são (até porque um deles foi preso por uma operação da PF em 2012, também por site de ódio), como eu fui tratada como suspeita. Foi esse caso que fez com que Luizianne (que ainda não conheço pessoalmente) apresentasse a proposta da Lei Lola.[21]

Verifica-se, portanto, que a importância da Lei se dá pela maior possibilidade de investigação dos crimes cometidos contra as mulheres, permitindo a adoção de instrumentos disponíveis para a Polícia Federal sem, contudo, retirar a competência das outras polícias do país.

Essas quatro leis específicas buscam proteger as mulheres no âmbito criminal na internet e, para além disso, também é possível visualizar outros instrumentos que permitem a retirada de conteúdo das redes, através do Marco Civil da Internet, bem como através dos próprios Termos de Uso dos provedores de internet. É o que se verificará a seguir.

4 OS PARÂMETROS DE REGULAÇÃO NO ÂMBITO CIVIL: O MARCO CIVIL DA INTERNET

Como visto, muitos dos atos ilícitos online envolvem a divulgação de conteúdos íntimos e, para além da responsabilização dos autores dessa prática criminosa, busca-se a retirada do conteúdo da internet. Sobre a responsabilização, havia uma dúvida sobre a possibilidade dos provedores de internet (como *Facebook, Twitter)* responderem por esse crime, bem como o seu papel na retirada do conteúdo

[21] ARONOVICH, Dolores. Lei Lola foi aprovada hoje. Disponível em <http://escrevalolaescreva.blogspot.com/2017/12/lei-lola-foi-aprovada-hoje.html>. Acesso em: 1 dez. 2020.

na rede. Isso em decorrência dos direitos constitucionais da liberdade de expressão e da manifestação de pensamento (art. 5º, IV e IX, CF), uma vez que não poderiam sofrer qualquer restrição (art. 220, CF), e o – aparente – conflito com o direito à reparação ao dano material, moral ou à imagem é assegurado, assim como é inviolável a intimidade, vida privada, honra e imagem das pessoas (art. 5º, V e X, CF).

Dessa forma, antes de entrar na efetiva questão da responsabilidade, resta, primeiro, entender os diferentes conceitos que o Marco Civil traz sobre os provedores: há aqueles provedores de aplicações de internet e provedores de conexão à internet. O provedor de aplicações é aquele que desempenha várias atividades na rede, enquanto o provedor de conexão apenas permite o acesso do usuário até a própria internet.

Desde o final dos anos 90, é pacífico o entendimento que provedores de conexão não são responsáveis pelas condutas de seus usuários. Isso porque, como visto, esse tipo de provedor apenas habilita um terminal para utilização da internet. Tecnicamente, seria impossível esse provedor evitar comportamentos danosos, a não ser que se implantasse um sistema de monitoramento em massa – o que não se deve perquirir. Mas não só isso.[22]

O acesso do usuário à internet não é a causa direta e imediata do dano que se causa à vítima, ao contrário, é o próprio comportamento do usuário que causa o dano[23]. Dessa forma, o Marco Civil da Internet, em seu art. 18, exclui a responsabilidade dos provedores de internet por danos de terceiros.

Ao provedor de aplicações de internet, todavia, o Marco Civil designa uma condição para que haja a responsabilização civil por danos de terceiros: apenas se, após ordem judicial específica, o provedor não tomar providencias para retirar o conteúdo. Veja-se o art. 19, que estabelece a regra e o procedimento para a incidência da responsabilidade civil dos provedores de internet:

> 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

[22] Ibidem, p. 98.
[23] Ibidem, p. 98

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

Cabe destacar que, objetivando um processo célere, o próprio MCI reconheceu que os conteúdos danosos aos direitos de personalidade podem ser apresentados perante juizados especiais, o que acaba por facilitar o percurso traçado por muitas mulheres que se sentem lesadas, seja com conteúdo sexual ou moral.

Um pouco mais a frente, em seu art. 21, o Marco Civil traz uma responsabilidade subsidiária aos provedores de aplicação por violação à intimidade, na exposição de materiais com cunho sexual e de caráter privado, caso deixe de promover a indisponibilização desse conteúdo. O contexto da inserção deste dispositivo se deu quando duas adolescentes cometeram suicídio após terem vídeos íntimos divulgados na internet, o que ocasionou comoção pública[24]:

> Art. 21. O provedor de aplicações de Internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da

[24] VALENTE, Mariana Giorgetti; NERIS, Natália; RUIZ, Juliana Pacetta; BULGARELLI, Lucas. O Corpo é o Código: estratégias jurídicas de enfrentamento ao revenge porn no Brasil. InternetLab: São Paulo, 2016.p. 75-77.

> divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.
>
> Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Aqui, cabem alguns apontamentos: a notificação deve ser feita pelo próprio participante ou representante legal; a notificação deve conter elementos para tornar possível a identificação do material apontado. Ou seja, o ônus da identificação do conteúdo é da vítima, assim como a responsabilidade de notificação. A norma, portanto, incentiva os provedores de aplicação a retirarem os conteúdos o quanto antes de suas plataformas, objetivando evitar maiores danos às vítimas: [25]

> Assim, ainda que esse assunto não tenha sido discutido nas consultas públicas prévias à elaboração final do Marco Civil, a lei nascia com uma regra específica de responsabilidade dos provedores de aplicação na Internet para os casos de imagens íntimas não consensuais (NCII), visando a incentivar as plataformas a remover o conteúdo o quanto antes, sem obrigar a vítima a cumprir formalidades, constituir advogado, ou buscar a Justiça.
>
> Se esse foi o objetivo declarado na edição da norma, o que é de se questionar é se os efeitos sobre o desenrolar dos casos foram sentidos. Em concreto, se a regra fez com que os provedores de aplicações se tornassem mais céleres na remoção dos conteúdos de nudez não consentida pelos participantes.

Carlos Affonso Souza nota que os dispositivos supracitados afastam a responsabilidade objetiva dos provedores, apontando para subjetiva. Ademais, subentende-se que, na regra geral (excetuando-se o art. 21), se os provedores tomarem ciência do conteúdo danoso de forma extrajudicial e não retiram o conteúdo ilícito, também não há responsabilidade. Lembre-se: incide a responsabilidade apenas com a negativa de se cumprir ordem judicial. Entretanto,

[25] Ibidem, p. 77

isso não significa que o Marco Civil apenas permita a retirada de conteúdo com ordem judicial[26]:

> O que o Marco Civil determina é a salvaguarda dos provedores de aplicações no sentido de que os mesmos apenas serão responsabilizados se não cumprirem ordem judicial para a retirada do material ofensivo. Isso não impede que os provedores possam determinar requisitos para a remoção de conteúdo em seus termos de uso e atendam eventuais notificações enviadas pelas supostas vítimas de danos decorrentes do conteúdo publicado.
>
> A adoção dessa medida visa a combater a indústria das notificações para remoção de conteúdo pelos mesmos argumentos apresentados anteriormente. O Marco Civil assume posição de defesa da liberdade de expressão e garante aos provedores a imunidade que neutraliza o temor que poderia existir no sentido de que a não remoção do conteúdo, depois da notificação, geraria a sua responsabilização.

Portanto, os provedores de aplicação da internet estão livres para determinar requisitos para a remoção de conteúdo em seus termos de uso. Pensando nisso, as linhas abaixo destinam-se a analisar os termos de uso de três provedores no que tange à remoção de conteúdo, principalmente numa perspectiva de gênero. Será que os provedores assumem esse papel social de forma espontânea?

5 OS PARÂMETROS DE REGULAÇÃO NO ÂMBITO PRIVADO: BREVE ANÁLISE DOS TERMOS DE USO DO TWITTER, FACEBOOK E INSTAGRAM

A breve análise apresentada abaixo dos Termos de Uso das redes sociais faz concluir que os provedores de aplicações usam do seu direito de retirada de conteúdo sem a necessidade de notificação judicial para cada remoção. Também se percebe que, mesmo sem denúncias por partes dos usuários, as plataformas se reservam no direito de excluir o conteúdo ou a conta de maneira espontânea. Veja-se:

5.1 Twitter

Analisando os Termos de Uso do Twitter, o tópico 5º tem como objeto "isenções e limitações de responsabilidade". Ali, é deixado bem claro que a

[26] SOUZA, Carlos Affonso; LEMOS, Ronaldo. Marco Civil da Internet Construção e Aplicação. Juiz de Fora, Editar, 2016. p. 100.

plataforma se exime de toda responsabilidade por integridade, confiabilidade, segurança dos serviços, ou a qualquer "perda intangível", resultante de conduta ou conteúdo incluindo material difamatório, ofensiva, ou ilegal de terceiros[27].

Sobre possíveis retiradas de conteúdo, verifica-se que plataforma permite denúncias contra assédio; ameaças diretas específicas de violência que envolvem integridade física ou bem-estar; informação ou foto particular exposta; spam; mensagem de ódio contra uma categoria protegida (por exemplo, raça, religião, gênero, orientação, deficiência). Ao selecionar o tipo de assédio, o twitter também pergunta se a natureza do comportamento se direciona "a mim", "alguém que represento legalmente", ou "dirigidos a outros (amigo ou um grupo).[28]

5.2 Facebook

O tópico 3º dos Termos de Uso do Facebook também traz os "limites da responsabilidade". Segundo o documento: "Não controlamos nem orientamos o que as pessoas e terceiros fazem ou dizem e não somos responsáveis pela conduta deles (seja online ou offline) ou por qualquer conteúdo que compartilham (inclusive conteúdo ofensivo, inadequado, obsceno, ilegal ou questionável)".[29]

Para oferecer denúncia dentro da plataforma, o Facebook informa que o conteúdo deve violar os Padrões da Comunidade. Assim, dentro do tópico "II. Segurança", consta exploração sexual, abuso ou nudez infantil; exploração sexual de adultos; bullying e assédio; exploração humana; violações de privacidade e direitos de imagem. Além disso, no tópico "III. Conteúdo questionável", está discurso de ódio; violência e conteúdo explícito; nudez adulta e atividades sexuais; abordagem sexual e outros.[30]

[27] Twitter. Termos de Uso. Disponível em <https://twitter.com/pt/tos>. Acesso em: 1 de out. 2020.
[28] Twitter. Denúncia por comportamento abusive ou assédio. Disponível em <https://help.twitter.com/forms/abusiveuser>. Acesso em 30 de set. 2020.
[29] Facebook. Termos de Uso. Disponível em <https://www.facebook.com/terms>. Acesso em: 1 de out. 2020.
[30] Facebook. Padrões da Comunidade. Disponível em <https://www.facebook.com/communitystandards/introduction>. Acesso em: 1 de out. 2020.

5.3 Instagram

Os Termos do Instagram tratam sobre "remoção de conteúdo e desativação ou encerramento da sua conta", onde a plataforma informa que poderá remover qualquer conteúdo ou informação compartilhada pelo usuário, se acreditarem que viola os Termos de Uso ou quando forem autorizados/obrigados por lei. Da mesma forma que os termos acima analisados, o Instagram também limita suas responsabilidades através do capítulo "Quem é responsável caso algo aconteça". Nesse tópico, afirma-se que não há a garantia da plataforma ser segura todo o tempo, que não há controle sobre o que terceiros fazem ou pelos seus serviços oferecidos.[31]

Na página de denúncias, em "Central de Privacidade e Segurança", há hipóteses de denúncias contra os discursos de ódio (assédio/bullying); crianças menores de idade; informações privadas expostas; exploração infantil; tráfico humano; entre outros.[32]

6 CONSIDERAÇÕES FINAIS

No percorrer desta pesquisa pode-se notar os principais parâmetros de regulação contra a violência de gênero na internet, no âmbito criminal, cível e privado. Como conclusão, depreende-se que o ordenamento jurídico está dotado de instrumentos para combater a violência contra a mulher no mundo virtual.

Mesmo que não pareça ser suficiente para coibir a reprodução das desigualdades de gênero na rede, a solução do problema não parece estar na tipificação de mais crimes – se assim fosse, a sociedade já teria atingido seu patamar de igualdade social. Além disso, quando se está a falar sobre internet, todo cuidado é pouco para que não haja vigilância em massa e obste o poder da população em se inserir nas redes.

No que tange aos parâmetros abordados no âmbito criminal e no âmbito cível, percebe-se que o Estado, mesmo com um certo "atraso", vem exercendo seu papel

[31] Instagram. Termos de Uso. Disponível em <https://www.facebook.com/help/instagram/581066165581870>. Acesso em: 1 de out. De 2020.

[32] Instagram. Denunciar algo. Disponível em: <https://help.instagram.com/122717417885747/?helpref=hc_fnav&bc[0]=Ajuda%20do%20Instagram&bc[1]=Central%20de%20Privacidade%20e%20Seguran%C3%A7a&bc[2]=Denunciar%20algo>. Acesso em: 1 out. 2020.

para regular as redes sem violar a liberdade de expressão. Já no âmbito privado, percebe-se que as plataformas analisadas exercem a possibilidade conferida pelo Marco Civil de retirarem conteúdos que violem seus Termos de Uso, mas percebeu-se uma falta de transparência em como são retirados conteúdos lesivos e quais os dados que se tem sobre isso.

REFERÊNCIAS

BACKES, Ana Luiza et al. Breve **Análise dos Dados sobre candidaturas de Mulheres nas Eleições de 2018. Estudo técnico. 2019.** Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/comissao-de-defesa-dos-direitos-da-mulher-cmulher/arquivos-de-audio-e-video/breve-analise-dos-dados-sobre-candidatas-eleitas-receitas-nas-eleicoes-de-2018> Acesso em: 7 de mar. 2020.

BARROSO, Luis Roberto. **Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação**. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. Revista de Direito Administrativo, Rio de Janeiro, v. 235, p. 1-36, jan. 2004. ISSN 2238-5177. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/45123/45026>. Acesso em: 29 Set. 2020.

BIROLI, Flávia. **Divisão Sexual do Trabalho e Democracia**. DADOS – Revista de Ciências Sociais, Rio de Janeiro, vol. 59, no 3, 2016. p. 726-727. Disponível em <http://www.scielo.br/pdf/dados/v59n3/0011-5258-dados-59-3-0719.pdf>.Acesso em: 12 de mar. 2020.

BITTENCOURT, Epaminondas. CARRIERI, Alexandre. **RESPONSABILIDADE SOCIAL: IDEOLOGIA, PODER E DISCURSO NA LÓGICA EMPRESARIAL**. eRAE. VoL. 45. Edição Especial Minas Gerais. 2005. Disponível em <https://www.scielo.br/pdf/rae/v45nspe/v45nspea01.pdf>. Acesso em: 2 de out. 2020.

CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros - TIC Domicílios 2017**. Inclui os usuários de Internet, os usuários de Internet no telefone celular e os usuários de aplicações que necessitam de conexão à Internet.

FACEBOOK. **Termos de Uso.** Disponível em <https://www.facebook.com/terms>. Acesso em: 1 de out. 2020.

FACEBOOK. **Padrões da Comunidade.** Disponível em <https://www.facebook.com/communitystandards/introduction>. Acesso em: 1 de put. 2020.

FOLHA. **Grupos em redes sociais incentivam necrofilia.** Disponível em <https://www1.folha.uol.com.br/cotidiano/2020/09/grupos-em-redes-sociais-incentivam-necrofilia.shtml>. Acesso em 1 de out. 2020.

IBGE. **Diferença do rendimento do trabalho de mulheres e homens nos grupos ocupacionais** - Pnad Contínua. 2018.

INSTAGRAM. **Termos de Uso**. Disponível em <https://www.facebook.com/help/instagram/581066165581870>. Acesso em: 1 de out. De 2020.

INSTAGRAM. **Denunciar algo**. Disponível em: <https://help.instagram.com/122717417885747/?helpref=hc_fnav&bc[0]=Ajuda%20do%20Instagram&bc[1]=Central%20de%20Privacidade%20e%20Seguran%C3%A7a&bc[2]=Denunciar%20algo>. Acesso em: 1 out. 2020.

Instituto ETHOS. **Conceitos Básicos e Indicadores de Responsabilidade Social Empresarial – 5ª edição**. 2007. Disponível em: <https://www.ethos.org.br/cedoc/conceitos-basicos-e-indicadores-de-responsabilidade-social-empresarial-5a-edicao-2/>. Acesso em 2 de out. 2020.

Instituto ETHOS. BORGER, Fernanda Gabriela. **Responsabilidade social empresarial e sustentabilidade para a gestão empresarial.** Disponível em <https://www.ethos.org.br/cedoc/responsabilidade-social-empresarial-e-sustentabilidade-para-a-gestao-empresarial/>. Acesso em 2 de out. 2020.

INTERNET WORLD STATS. Disponível em <https://www.internetworldstats.com>. Acesso em: 28 de set. 2020.

LIMONGI, Fernando; OLIVEIRA, Juliana de Souza; SCHMITT, Stefanie Tomé**. Sufrágio universal, mas... só para homens. O voto feminino no Brasil**. Revista de Sociologia e Política v. 27, n. 70, 2019, p. 18. Disponível em <https://www.scielo.br/pdf/rsocp/v27n70/0104-4478-rsocp-27-70-e003.pdf>. Acesso em: 3 de jun. 2020.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco Civil da Internet Construção e Aplicação**. Juiz de Fora, Editar, 2016.

TWITTER. Termos de Uso. Disponível em <https://twitter.com/pt/tos>. Acesso em: 1 de out. 2020.

TWITTER. **Denúncia por comportamento abusivo ou assédio**. Disponível em <https://help.twitter.com/forms/abusiveuser>. Acesso em 30 de set. 2020.

VALENTE, Mariana Giorgetti; NERIS, Natália; RUIZ, Juliana Pacetta; BULGARELLI, Lucas. **O Corpo é o Código: estratégias jurídicas de enfrentamento ao revenge porn no Brasil**. InternetLab: São Paulo, 2016.

INFILTRAÇÃO POLICIAL COMO FORMA DE INVESTIGAR OS CRIMES SEXUAIS COMETIDOS CONTRA CRIANÇAS E ADOLESCENTES

Nathan Vinagre Augusto dos Santos[1]

RESUMO

O presente artigo analisa a questão da infiltração policial na internet como forma de combater os crimes sexuais cometidos contra criança e adolescentes. Nisso, foi constado que o meio digital propiciou o aumento dos referidos delitos, bem como a criptografia da rede dificultava o rastreio do infrator. Assim, a infiltração virtual permitiria que policial adentrasse nas redes privadas como se delinquente fosse obtendo as provas incriminadoras. Destarte, foi evidenciado a efetividade da infiltração policial inclusive no combate aos crimes cometidos na Deep Web.

Palavras-chave: Crimes Sexuais. Criança e Adolescente. Infiltração Policial Virtual.

ABSTRACT

This article analyzes the issue of police infiltration of the Internet as a way to combat sexual crimes committed against children and adolescents. It was found that the digital environment has led to an increase in these crimes, and that the network's cryptography makes it difficult to track the offender. Thus, virtual infiltration would allow police officers to enter private networks as if they were criminals, and obtain incriminating evidence. Thus, the effectiveness of police infiltration was evidenced, including in combating crimes committed on the Deep Web.

Key words: Sexual Crimes. Child and Teenager. Virtual Police Infiltration.

1 INTRODUÇÃO

Com o advento da tecnologia e da internet, as sociedades passaram por uma espécie de adaptação ao mundo virtual que vinha sendo implantado. A conexão

[1] Bacharel em Direito pela Centro Universitário de Brasília. Aluno do curso de Pós-graduação Lato Sensu do Centro Universitário de Brasília – UniCEUB/ICPD. E-mail: nathan.vinagre@sempreceub.com

social, atualmente, apresenta-se cada vez mais virtualizada, não sendo necessário o contato físico para que duas ou mais pessoas possam dialogar e transferir mensagens e conhecimentos. A facilidade de comunicação e transmissão de informação na internet proporcionou a criação de todo um "mundo" virtual, conectando diversas pessoas de diferentes nações.

A capacidade de transmissão de dados e comunicação pessoal no meio digital, infelizmente, atraiu a atenção de diversos infratores que verificaram a rede de computadores como uma forma de cometimento de delitos sem o risco expositivo. Diante disso, diversos crimes começaram a ser praticados por intermédio da internet, utilizando-se da disponibilidade de comunicação de forma anônima.

Somando-se a isso, temos uma crescente utilização da rede por crianças e adolescentes, participando intensivamente em diversos aplicativos e redes socias. A facilidade de comunicação com público infanto-juvenil, por intermédio da rede mundial de computadores, permitiu que diversos criminosos conseguissem manter uma ponte de contato com a vítima sem a ciência dos responsáveis legais.

A manipulação da mente do jovem, menor de idade, é uma coisa recorrente nos delitos sexuais praticados contra vulneráveis, sendo de difícil constatação, dada a impossibilidade de descoberta do fato delituoso, uma vez que a vítima é única pessoa que sabe sobre o ato. Cada vez mais, os agentes dos delitos sexuais envolvendo menores vem desenvolvendo formas de evitar o rastreio, sendo dificilmente identificada a autoria delitiva pela autoridade policial, o qual, inclusive, somente toma ciência da ocorrência do crime quando a vítima pronuncia-se sobre o fato.

Frente a essa dificuldade operacional para constatar tanto a autoria como a materialidade delitiva, o ordenamento jurídico e autoridade policial começaram a desenvolver técnicas para o enfrentamento da infração. Um desses instrumentos de investigação que vem sendo amplamente estudado e aprimorado consiste na infiltração policial nas redes de informática, a fim de captar o momento exato da ocorrência do delito, bem como desvendar o autor do fato delituoso por rastreio dos aparelhos utilizados e redes conectadas.

Diante disso, surgem diversos questionamentos referente a infiltração policial na rede. Como o policial deve proceder para infiltrar-se em caso de delitos sexual praticado contra pessoas ditas vulneráveis? Qual seria, observando as regras descritas no ordenamento jurídico, o procedimento adequado para tanto? Como selecionar o grupo de policiais a se infiltrar na rede virtual? Como seria a questão da fabricação de uma identidade falsa para a facilitar a infiltração? Dentre outros questionamentos que possam advir desse método investigativo.

Para solucionar as referidas questões, faz-se imprescindível verificar a procedibilidade da infiltração policial, utilizando-se de acervo bibliográfico contendo as informações sobre a referida medida. Além disso, seria necessário observar o grau de êxito da técnica investigatória adotada em operações policiais anteriores. Em suma, o presente artigo buscará analisar a questão da infiltração policial para a investigação de crimes sexuais cometidos nas redes virtuais de computadores, a fim de constatar a sua viabilidade probatória.

2 CRIMES SEXUAIS COMETIDOS CONTRA VULNERÁVEIS NOS MEIOS VIRTUAIS

A utilização da rede mundial de computadores tornou-se algo frequente na sociedade moderna. Milhares de usuários utilizam seus aparelhos conectados à internet, com finalidade de percepção e emissão da informação. A internet tornou-se tão arraigado na sociedade que, modernamente, as crianças, de forma prematura, desenvolvem a capacidade de interagir na rede como se fosse algo extremamente natural.

Apesar do caráter positivo da internet como a transmissão constante de informação a cada milésimo de segundo, a rede trouxe diversas consequências negativas. A utilização descontrolada e sem fiscalização da rede por crianças e adolescentes permitiu a atuação de diversos infratores que verificaram o mundo digital como um ponto de cometimento de delitos sexuais contra os menores. Vale frisar que a culpa dos atos imorais não é da rede em si, mas sim da sua movimentação, com clara finalidade ilícita, por seres humanos.

A prática de crimes envolvendo a dignidade sexual de crianças e adolescentes, ao longo dos tempos, é um fator recorrente na sociedade, devendo ser amplamente combatida.[2] Acontece que o advento da internet e a facilidade de comunicação entre pessoas maximizou a ocorrência dos referidos delitos, permitindo que o infrator consiga praticar os atos delituosos de forma mais acessível e em anonimato. Atualmente, diversas crianças e adolescentes possuem em seus lares acesso a computadores com webcam, celulares, entre outros capazes de transmitir imagens e comunicações, o que facilitaria a atuação do infrator, com a finalidade de obtenção de favores de cunho sexual de menores vulneráveis.[3]

Corroborando com isso, os menores incapazes possuem uma mentalidade amplamente suscetível a manipulação externa, dada a sua incompleta formação psíquica. Diante disso, os infratores, utilizando-se de métodos indutivos, estimulam o jovem incapaz a compartilhar fotografias, vídeos, imagens de cunho sexual, com o objetivo de saciar a sua lasciva.[4] Portanto, um dos modus operandi das infrações sexuais contra menores nas redes constituem na manipulação psíquica da mente em formação da criança para obtenção de material pornográfico. Nesse sentido, na era digital, ficou muito comum a denúncia dos chamados crimes contra dignidade sexual dos jovens vulnerável, devendo o menor receber uma proteção especial por parte do ordenamento jurídico, a fim de conter o referido delito.

Vale frisar que os crimes sexuais a serem cometidos contra o público infanto-juvenil estão inseridos tanto no Código Penal como no Estatuto da Criança e Adolescente. Nesse sentido, a conduta do infrator pode ser enquadrada em diversos crimes digitais que vão desde a obtenção/armazenamento de dados até o efetivo encontro presencial da criança com o delinquente. Porém, o objetivo do presente artigo é tratar da infiltração policial para o combate do referido delito, ou seja, não será esmiuçado cada tipo penal dos delitos praticados contra crianças e adolescentes

---

[2] CAVALCANTE, Laylana Almeida de Carvalho. Ciberpedofilia: crimes sexuais contra crianças e adolescentes praticados através da internet. **Research, Society and Development**, v. 9, n. 2, p. 23, 2020.

[3] PIRES, Luiza Matias. A infiltração policial virtual nos crimes contra a dignidade sexual da criança e do adolescente: análise da infiltração sob a ótica da lei 13.441/17. **ISSN 1677-1281**, v. 36, n. 36, 2018.

[4] CAVALCANTE, Laylana Almeida de Carvalho. Ciberpedofilia: crimes sexuais contra crianças e adolescentes praticados através da internet. **Research, Society and Development**, v. 9, n. 2, p. 23, 2020.

na rede, se atendo mais ao número de infrações cometidos acrescido da forma como os autores atuam para o cometimento dos delitos.

2.1 Pedofilia cometida na rede mundial de computadores em número

A pedofilia constitui um transtorno mental, sendo uma espécie de parafilia, a qual a pessoa sente atração sexual por crianças e adolescentes.[5] Não há um tipo penal propriamente que define o crime de pedofilia, mas sim há a previsão de condutas esparsas que podem ser enquadrados no referido conceito.[6] Assim, o Código Penal e o Estatuto da Criança e Adolescente não utilizaram o nome pedofilia para a definição do crime, sendo, então, a referida nomenclatura utilizada popularmente para se referir a diversas condutas contrarias a dignidade sexual da criança e do adolescente.

Consoante pesquisa realizada pela TIC Kids Online, foram detectados, em 2019, que 89% da população entre 9 e 17 anos possuem acesso à internet, o que em números corresponderia, aproximadamente, a 24 milhões de crianças e adolescentes.[7] Dentre os referidos números, apenas 77% dos pais ou responsáveis dos menores vulneráveis supervisionam as crianças nos momentos em que elas utilizam a internet.[8] Nesse sentido, é possível verificar que 33% dos responsáveis legais não fiscalizam os conteúdos que seus filhos tem acesso, o que significa dizer que tais crianças apresentam maior probabilidade de vir a ser vítima de crimes contra dignidade sexual.

---

[5] CARVALHO, Lucas Machado. A prática da Pedofilia e Crimes Sexuais: A aplicação da Lei em Crimes Virtuais. Monografia apresentada à Universidade Católica de Goiás. 2020. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/955/1/LUCAS%20MACHADO%20CARVALHO.pdf. Acesso em: 28 set 2021.

[6] CARVALHO, Lucas Machado. A prática da Pedofilia e Crimes Sexuais: A aplicação da Lei em Crimes Virtuais. Monografia apresentada à Universidade Católica de Goiás. 2020. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/955/1/LUCAS%20MACHADO%20CARVALHO.pdf. Acesso em: 28 set 2021.

[7] Comitê Gestor da Internet do Brasil. Resumo executivo: pesquisa TIC kids online brasil 2019. Disponível em: https://cetic.br/media/docs/publicacoes/2/20201123093441/resumo_executivo_tic_kids_online_2019.pdf. Acesso em: 28 set 2021.

[8] Comitê Gestor da Internet do Brasil. Resumo executivo: pesquisa TIC kids online brasil 2019. Disponível em: https://cetic.br/media/docs/publicacoes/2/20201123093441/resumo_executivo_tic_kids_online_2019.pdf. Acesso em: 28 set 2021.

A prática de conduta descrita como crimes contra a dignidade sexual pode ser exercida por diversos meios dentro das redes virtuais. As mais comuns constituem na hospedagem de sites de pornografia infantil. O agente do delito interage com crianças e adolescentes, adquirindo conteúdo de caráter sexual e consequentemente alimentando o site ilícito. Segundo dados divulgados pela ONG SaferNet Brasil, em 2021 houve um crescimento de 33,45% de denúncias de sites contendo pornografia infantil,[9] fato esse acarretado pelo alto uso da rede mundial de computadores durante a pandemia de COVID-19.

Em 2020, no período correspondente ao início do estado pandêmico, foram contabilizados pela ONG 98.244 denúncias referentes a existência de sites contendo pornografia infantil, sendo mais que o dobro do período correspondente ao ano de 2019, o qual contabilizava 48.576 denúncias.[10] Por outro lado, somente considerando os meses de janeiro até abril, a SaferNet Brasil contabilizou 15.856 denúncias, "das quais 7.248 foram removidas por indício de crime".[11] Ao todo, durante o lapso temporal de 15 anos desde o início da contagem de crimes envolvendo a hospedagem de site contendo pornografia infantil, foram constatadas 1.759.354 denúncias anônimas de pornografia infantil referente a 429.665 páginas distintas, tendo sido removidas 340.005 por crimes.[12]

A pandemia como um todo estabeleceu que as crianças necessitavam acessar a rede mundial de computadores para assistir as suas respectivas aulas escolares. Entretanto, a internet é uma rede vasta com diversas formas de comunicação interpessoais, o que tornou mais acessível o seu uso desenfreado, facilitando a interação de um agente delinquente com o jovem vulnerável. Portanto, o aumento

[9] SAFERNET. Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta a Safernet Brasil. 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil. Acesso em: 28 set 2021.

[10] SAFERNET BRASIL. Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta a Safernet Brasil. 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil. Acesso em: 28 set 2021.

[11] SAFERNET BRASIL. Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta a Safernet Brasil. 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil. Acesso em: 28 set 2021.

[12] SAFERNET BRASIL. Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta a Safernet Brasil. 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil. Acesso em: 28 set 2021.

das incidências de delitos contra dignidade sexual era algo, praticamente, inevitável, restando, então, a efetiva investigação e punição dos indivíduos que o cometeram.

Novamente, vale reverberar que não é responsabilidade da rede o controle referente ao acesso das crianças, o problema de divulgação de conteúdo indevido é de culpa exclusiva do real infrator. Todos os instrumentos, por mais bem intencionados e úteis que forem, podem ser utilizados para cometimento de delitos, sendo que o mundo digital não escapa da referida regra. Destarte, não se deve realizar uma censura prévia do instrumento e sim deve-se combater e punir os reais delinquentes.

Outro ponto importante a ser elucidado consiste na dificuldade de precisar a quantidade de delitos contra dignidade sexual cometidos contra menores vulneráveis. Como o delito é praticado no âmbito privado da rede, a autoridade judiciária e policial somente saberá a ocorrência do fato criminoso quando a vítima resolve se pronunciar sobre o ocorrido, o que significa dizer que as denúncias normalmente são realizadas de formas tardias.[13]

Além disso, no Brasil, como os crimes ocorrem em estados federais diversos não há uma unificação de informação, tornando nefastos os dados envolvendo os delitos cometidos nas redes. Destarte, o presente artigo buscou apresentar os dados disponíveis pelos órgãos públicos e ONGs referentes aos sites de pornografia infantil, o qual tende a concentrar a maior parte dos delitos cometidos contra crianças e adolescentes, ou seja, quando alguém adquire conteúdo de cunho sexual envolvendo menores, eles costumam postar e divulgar em sites ilícitos. Por esse motivo, acredita-se que a quantidade de delitos de caráter sexual contra menores nas redes, estimativamente, tende a ser maior muito maior do que os dados efetivamente divulgados.

[13] CAVALCANTE, Laylana Almeida de Carvalho. Ciberpedofilia: crimes sexuais contra crianças e adolescentes praticados através da internet. **Research, Society and Development**, v. 9, n. 2, p. 23, 2020.

2.2 Da dificuldade investigatória nas redes virtuais

Os crimes cometidos pelos meios digitais, apesar de serem passíveis de rastreamento do endereço de IP, são normalmente realizados em situações que dificultam a investigação. Primeiramente, para que haja a efetiva investigação referente ao crime cometido contra crianças e adolescentes, é necessário que a informação do ocorrido chegue até o delegado de polícia. Diante disso, o início investigatório começa de forma tardia, somente sendo relatado o ocorrido transpassado um lapso temporal extenso do fato delituoso.[14] Nesse sentido, embora ainda seja possível para autoridade policial desvendar o infrator, tal demora eleva a dificuldade em solucionar a referida infração.

Os delinquentes, no âmbito do cometimento do delito, buscam, a todo momento, apagar seus rastros, para evitar uma possível identificação. Apesar da comunicação inicial entre o infrator e a criança começar, em alguns casos, na rede social, o agente do delito utiliza-se de perfil falso bem como de conexões de internet alheia, de acesso gratuito, como é o caso de restaurantes, hotéis, etc., para adquirir o conteúdo de caráter ilícito, buscando sempre descartar o aparelho utilizado na conexão.[15] Com isso, o rastreio do perfil torna-se uma tarefa difícil, dado a divergência dos pontos de acesso a rede mundial de computadores, tendo que ter uma análise profunda das câmeras de segurança com a finalidade de localizar o indivíduo que coincidentemente esteve presente em todos os pontos de acesso no horário específico ao do momento em que a infração foi cometida.

Ao adquirir o conteúdo sexual de caráter ilícito, o qual pode advir de diversas fontes (tais quais a venda de crianças pelos responsáveis, sequestro, manipulação na rede social para conseguir determinadas fotos, entre outros) a divulgação do material

[14] TELES, Ketlhen Rayane Nunes de Sá. Crimes virtuais de pornografia infantojuvenil e pedofilia: um estudo sobre os fluxos de investigações. Centro Universitário FG. Guanambi. Bahia. 2021. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/13478/1/TCC%20II%20FINALIZADO%20KETLHEN%20RAYANE%20NUNES%20DE%20S%c3%81%20TELES.pdf. Acesso em 28 set 2021.

[15] TELES, Ketlhen Rayane Nunes de Sá. Crimes virtuais de pornografia infantojuvenil e pedofilia: um estudo sobre os fluxos de investigações. Centro Universitário FG. Guanambi. Bahia. 2021. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/13478/1/TCC%20II%20FINALIZADO%20KETLHEN%20RAYANE%20NUNES%20DE%20S%c3%81%20TELES.pdf. Acesso em 28 set 2021.

se dá por intermédio de uma rede oculta que dificulta o rastreio, conhecido como Deep Web.[16]

A internet como um todo pode ser dividida em duas classificações, sendo uma delas a Superface Web, o qual consiste na parte acessível ao público em geral pelos programas de navegação simples.[17] Nesse sentido, o sistema de busca simples da internet, Google, Yahoo, etc., utilizam indexação de dados e arquivos de caráter público, permitindo o acesso por qualquer pessoa pela mera pesquisa.[18]

Entretanto, existe uma segunda parte da rede mundial de computadores chamada de Deep Web com dados não registrados, que necessitam de ferramentas especiais para que possam ser acessadas. Dentro da camada obscura da internet, é possível verificar a existência de conteúdos que somente podem ser visualizados através de programas específicos, sendo chamada de Dark Web, o qual somente pode ser acessada por meio de navegadores especiais, como é o caso do TOR (The Onion Route).[19] Destarte, a rede oculta nada mais seria do que uma concentração de arquivos não catalogados e de difícil percepção pelo usuário, tornando-se um meio para a divulgação de delitos realizados pelo agente, tais quais a criação de site contendo pornografia infantil, venda de crianças sequestradas, etc.

O rastreio dos indivíduos que utilizam o programa TOR para acessarem a Dark Web é extremamente complicado. Tal ferramenta distribui a conexão do usuário com diversas redes de voluntários, o que significa dizer que a conexão passa por diferentes camadas de redes, sendo que cada uma delas auxilia a criptografar tráfego do computador.[20] O monitoramento do usuário, para desvendar a pessoa

---

[16] DE MATTOS, Kennedy Josué Greca. Crimes praticados na dark web e a dificuldade de resposta estatal. 2020. https://www.unifor.br/documents/392178/3101527/Kennedy+Josue+Greca+de+Mattos.pdf/fbab6502-5e60-b2e1-8d57-1b29fd65ba05. Acesso em: 28 set 2021.

[17] ÂNGELO, Luíza Alice Torres. Crimes cibernéticos: as limitações da resposta estatal a criminalidade informática. 2017. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/11418/1/LATA07062017.pdf. Acesso em: 28 set 2021.

[18] SATO, Gustavo Worcki. A infiltração virtual de agentes e o combate à pedopornografia digital: estudo da lei 13.441/2017 e lei 13.964/2019. **J²-Jornal Jurídico**, v. 4, n. 1, p. 163-181, 2021.

[19] ÂNGELO, Luíza Alice Torres. Crimes cibernéticos: as limitações da resposta estatal a criminalidade informática. 2017. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/11418/1/LATA07062017.pdf. Acesso em: 28 set 2021.

[20] DE MATTOS, Kennedy Josué Greca. Crimes praticados na dark web e a dificuldade de resposta estatal. 2020. Disponível em:

física, autora do delito, torna-se uma tarefa quase que impossível, uma vez que seria necessário decodificar diversos meios de acesso utilizados pelo agente, a fim de conseguir obter provas de autoria delitiva.

Para tal solução, os delegados de policiais, com os auxílios de especialistas na área da computação, catalogam todos os acessos de redes efetuados pelo usuário, mantendo a integra de todos os arquivos desvendados. Com isso, a autoridade policial busca justamente a identificação do enderença de IP, montando provas robustas referentes a autoria delitiva. Porém, tais tentativas mostram-se muitas vezes infrutíferas, sendo necessário a adoção de novas técnicas, a fim de atrair o infrator para fora da Deep Web mediante a utilização de técnicas que o enganam, como é o caso da infiltração policial na rede.

3 INFILTRAÇÃO POLICIAL NOS MEIOS DIGITAIS

Os crimes cometidos nas redes virtuais são sempre de difícil identificação, o que demandam a aplicação de técnicas investigativas com a finalidade de desvendar a autoria e materialidade delitiva. Uma das hipóteses recentemente integrada pela Lei 13.441/2017, o qual modificou o Estatuto da Criança e Adolescente, consiste na possibilidade de agente policial se infiltrar nos meios digitais, a fim de adquirir provas incriminadoras.

A referida metodologia investigativa nada mais seria do que a infiltração do agente policial, por intermédio de decisão judicial, em uma organização criminosa ou grupo, com a finalidade de adquirir as informações de suas estruturas.[21] O policial, assim, utilizando-se de um disfarce, enturma-se com os delinquentes para investigar o método de atuação da organização, hierarquia, os delitos já praticados, os futuros atos e planos da organização criminosa, etc. Todas as informações

https://www.unifor.br/documents/392178/3101527/Kennedy+Josue+Greca+de+Mattos.pdf/fbab6502-5e60-b2e1-8d57-1b29fd65ba05. Acesso em: 28 set 2021.

[21] JOSÉ, Maria Jamile. **A infiltração policial como meio de investigação de prova nos delitos relacionados à criminalidade organizada**. 2010. Tese de Doutorado. Universidade de São Paulo. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-01122010-144008/publico/Infiltracao_policial_Maria_Jamile_Jose.pdf. Acesso em: 28 set 2021.

referentes ao meio em que o agente se infiltrou são levantados, dando robusteza ao inquérito policial.[22]

Vale evidenciar que a infiltração desencadeia a necessidade de o policial esconder a sua identidade, enturmar-se com os infratores e atuar como se delinquente fosse.[23] Diante disso, o mero ato de adentrar na Dark Web com o objetivo de verificar os sites que ali se encontram não é considerado como a efetiva infiltração do policial, não sendo necessário a autorização policial, por exemplo. Portanto, o agente policial pode realizar algo semelhante como as "rondas" dentro da rede de forma preventiva, sem que isso seja identificada como a adoção do referido mecanismo investigatório.

A infiltração do agente policial não é um método investigativo recém-descoberto, sendo amplamente praticado em diversos países como Estados Unidos, Inglaterra e membros da União Europeia, etc., ganhando notoriedade pelo mundo. No Brasil, infiltração como forma de investigação somente foi previsto na Lei 10.217/2001, revogada pela Lei 12.850/13, sendo restrito apenas a organização criminosa.[24] Posteriormente, com a Lei 11.343/2006, houve a possibilidade da atuação do policial disfarçado nos crimes de tráfico de drogas. Por fim, como dito anteriormente, a modificação do ECA pela Lei 13.441/2017, reconheceu a necessidade de atuação do agente infiltrado na rede como forma de combater os delitos virtuais.

A recente legislação contendo a possibilidade de infiltração policial nos meios digitais apenas expandiu o rol de crimes que permitiam tal procedimento investigativo. Não houve uma inovação, por parte legal, nos procedimentos a serem

---

[22] BINI, Adriano Krul. **O agente infiltrado:** perspectivas para a investigação criminal na contemporaneidade. 2017. Dissertação de Mestrado da Instituto Superior de Ciências Policiais e Segurança Interna – ISCPSI. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/25429/1/DISSERTA%C3%87%C3%83O%20FINAL%20%20%20ap%C3%B3s%20j%C3%BAri.pdf. Acesso em: 28 set 2021.

[23] COSTA JÚNIOR, José Carlos Teixeira. Limites da Infiltração Policial na Internet e a Invasão de Dispositivo Informático: O advento da Lei 13.441/2017. Trabalho de Conclusão de Curso na Universidade Federal da Bahia. Salvador. 2018. Disponível em: https://repositorio.ufba.br/ri/bitstream/ri/26249/1/Jos%c3%a9%20Carlos%20Teixeira%20Csta%20J%c3%banior%20-%20Infiltra%c3%a7%c3%a3o%20policial%20na%20Internet%20e%20o%20crime%20do%20art.%20154-A.pdf. Acesso em: 28 set 2021.

[24] PIRES, Luiza Matias. A infiltração policial virtual nos crimes contra a dignidade sexual da criança e do adolescente: análise da infiltração sob a ótica da lei 13.441/17. **ISSN 1677-1281**, v. 36, n. 36, 2018.

adotados na infiltração dos agentes, assim, o método investigativo se respalda nos mesmos regramentos aplicados na Lei de Organização Criminosa.[25] A única diferença apresentada pela Lei 13.441/2017 seria a prática virtual da infiltração, sem que o agente precisasse encontrar presencialmente os delinquentes. Entretanto, apesar do procedimento de infiltração ser virtualizado não significa dizer que o policial não precisará atuar de forma presencial. A fim de ganhar confiabilidade do grupo praticante do delito, é imprescindível o comparecimento do agente disfarçados nas reuniões da organização praticante do delito.

Apesar a referida lei apresentar a modalidade digital na infiltração policial, tal mecanismo já vinha sendo adotado no Brasil para o combate dos crimes sexuais antes da sua vigência. A Lei 12.850/13 estipulava que a infiltração policial, também, poderia ser aplicada para a investigação de crimes previstos em convenções internacionais. Com isso, a Convenção Internacional sobre os direitos das crianças de 20 de novembro de 1989 determinava a repressão a exploração sexual infantil, permitindo assim, através da interpretação do art. 1º, §2º, incisos I e II da lei 12.850/13, a adoção da infiltração digital para o combate desses delitos.[26]

Vale ressaltar, também, que a Lei 13.964/2019 expandiu as hipóteses de infiltração virtual do policial, ao permitir que o agente se adentre virtualmente em qualquer organização criminosa, desde que haja autorização judicial.[27] Nesse sentido, em todos os crimes com pena máxima superior a quatro anos praticados por um grupo organizado com divisão hierárquica passível de classificação como organização criminosa, poderia ser adotada a infiltração digital do agente policial.

Embora haja essa previsibilidade legal do referido procedimento investigativo para qualquer organização criminosa, o presente artigo buscou limitar o estudo a infiltração para o combate de crimes sexuais praticados contra crianças e adolescentes. Por esse motivo, o capítulo em evidência abordará os requisitos para

[25] PEREIRA, Flávio Cardoso. Agente Infiltrado Virtual (Lei n. 13.441/17): Primeiras impressões. **Revista do Ministério Público do Estado de Goiás**, v. 97, 2017. Disponível em: http://www.mp.go.gov.br/revista/pdfs_12/8-ArtigoFlavio_Layout%201.pdf. Acesso em: 28 set 2021.

[26] RODRIGUES, Felipe José Sousa; CARDOSO, Sarah de Araújo Mendes; MARWELL, Tatiana Eulálio Dantas Guedes. Utilização da infiltração virtual nas operações policiais para o combate aos crimes sexuais contra crianças e adolescentes. **Research, Society and Development**, v. 10, n. 4, p. e24710414152-e24710414152, 2021.

[27] SATO, Gustavo Worcki. A infiltração virtual de agentes e o combate à pedopornografia digital: estudo da lei 13.441/2017 e lei 13.964/2019. **J²-Jornal Jurídico**, v. 4, n. 1, p. 163-181, 2021.

sua adoção e a eficiência do mecanismo investigatório, traçando sempre parâmetros de procedibilidade.

3.1 Dos requisitos legais e doutrinários para o deferimento da infiltração policial

O art. 190-A e seguintes do Estatuto da Criança e Adolescente (ECA) estabelecem os parâmetros para a adoção da infiltração policial como forma de investigação no inquérito, podendo inclusive ser complementada pelos ensinamentos constantes na Lei de Organização Criminosa.

Inicialmente, vale apontar que o referido instrumento investigativo não é passível de aplicação em qualquer delito praticado pelo agente, determinando um rol taxativo para a sua efetivação. Diante disso, somente os crimes praticados contra a dignidade sexual da criança e adolescente, previstos nos arts. 240 , 241 , 241-A , 241-B , 241-C e 241-D do ECA e nos arts. 154-A , 217-A , 218 , 218-A e 218-B do Código penal,[28] permite a infiltração no meio digital. O referido rol, com a entrada em vigor do Pacote Anticrime (Lei 13.964/2019), foi expandido para englobar qualquer crime praticado por intermédio de organização criminosa.

A identificação do delito praticado pelo agente é indispensável para que seja adotada a infiltração policial como meio de prova. O referido mecanismo sempre vem acompanhada da quebra da intimidade do investigado.[29] A violação de um direito fundamental, como é o caso da privacidade dos indivíduos, somente poderiam ser afastados mediantes a demonstração de sobreposição do interesse público ao privado, ou seja, somente quando o crime praticado possuir uma gravidade exacerbada que a justifique.

Ademais, nota-se que o agente policial fará um relatório detalhada de todos os atos praticados pelos suspeitos, com a finalidade de enquadrá-los nos delitos penalmente previstos e para evitar abusos do agente público. Como o referido

---

[28] BRASIL. Lei 8.069. Estatuto da Criança e Adolescente. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm#art240. Acesso em: 28 set 2021.

[29] BINI, Adriano Krul. **O agente infiltrado:** perspectivas para a investigação criminal na contemporaneidade. 2017. Dissertação de Mestrado da Instituto Superior de Ciências Policiais e Segurança Interna – ISCPSI. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/25429/1/DISSERTA%C3%87%C3%83O%20FINAL%20%20%20ap%C3%B3s%20j%C3%BAri.pdf. Acesso em: 28 set 2021.

instrumento probatório constitui uma quebra da privacidade dos suspeitos, somente haveria a motivação idônea para a infiltração policial se existisse provas minimamente também robustas no que diz respeito a materialidade e autoria delitiva, caso contrário estaríamos sujeitos a violação no âmbito privado sempre que Estado assim desejasse.[30]

Por esse motivo, o deferimento da referida prova se faz mediante autorização judicial, ante o requerimento do Ministério Público ou representação do delegado de polícia, sendo crucial a demonstração de indícios mínimos de autoria e materialidade delitiva, bem como da tipificação da conduta do agente em um crime socialmente reprovável. Além disso, para que não haja extensão excessiva da violação de privacidade, o mecanismo investigativo somente poderia perdurar por um prazo de 90 dias com possibilidade, mediante a efetiva demonstração da necessidade por decisão fundamentada, de sucessivas prorrogações, desde que não ultrapassem 720 dias.[31]

Corroborando com a necessidade e preservação dos direitos fundamentais, o ECA, em seu artigo 190-A, §3º, estabelece o caráter subsidiário da infiltração policial.[32] O referido meio de prova somente poderá ser deferido pelo magistrado quando inexistem outros meios de prova aptas fundamentar eventual condenação penal. Porém, dessa previsão legal advém o seguinte questionamento: como conciliar a necessidade de indícios de materialidade e autoria com a impossibilidade de comprovação do ato pelos demais meios de prova?

Tal questionamento pode ser solucionado da seguinte forma. Os indícios para que haja o deferimento da infiltração policial precisam ser mínimos, ou seja, basta que haja comprovação de cometimento de ato delituoso por parte de um grupo para que haja o deferimento do instrumento investigatório. Nesse contexto, a

---

[30] PEREIRA, Flávio Cardoso. Agente Infiltrado Virtual (Lei n. 13.441/17): Primeiras impressões. **Revista do Ministério Público do Estado de Goiás**, v. 97, 2017. Disponível em: http://www.mp.go.gov.br/revista/pdfs_12/8-ArtigoFlavio_Layout%201.pdf. Acesso em: 28 set 2021.

[31] ALMEIDA, Keslller Cristina Silva de. Infiltração policial no âmbito virtual como meio extraordinário de investigação criminal. Monografia apresentada à Universidade Federal do Paraná. Curitiba. 2019. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/68068/Monografia%20-%20Keslller%20Cristina%20Silva%20de%20Almeida%20%282019%29.pdf?sequence=1&isAllowed=y. Acesso em: 28 set 2021.

[32] BRASIL. Lei 8.069. Estatuto da Criança e Adolescente. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm#art240. Acesso em: 28 set 2021.

impossibilidade de demonstração pelos demais meios de provas apresentam a característica da especificidade, ou seja, necessita de indícios mais robustos para fundamentar eventual condenação além dos já apresentados no inquérito policial.

A título exemplificativo, imagine que determinado inquérito policial apresenta um boletim de ocorrência da vítima e de seu responsável com a narrativa do fato delituoso, sendo realizado uma investigação na qual foi desvendado um site composto de materiais que coincidem com o depoimento da vítima. Nisso, a autoridade policial tentou rastrear o responsável pelo site se deparando com vários endereços de IP diversos, o que caracterizaria a atuação de mais de um agente movimentando determinado site, mas não se tem certeza sobre quantos são os integrantes do grupo e nem como eles conseguiram todo aquele conteúdo pornográfico infantil. Destarte, existe provas de materialidade, bem como indícios mínimos de autoria, restando verificar a forma como os atos foram cometidos a fim de desvendar a totalidade de delitos praticados pelos agentes, sendo viável a utilização do agente infiltrado.

Por fim, a infiltração policial deve vir acompanhado da demonstração de êxito da operação. Ao realizar o requerimento, o Ministério Público ou delegado de polícia deve descrever, de forma fundamentada, a necessidade da infiltração policial, informando a possibilidade de obter resultados com o referido ato.[33] É possível verificar que nem sempre a infiltração do agente poderia auxiliar na obtenção probatória, impossibilitando o deferimento da referida prova.

Para tanto, seria necessário verificar, por exemplo, o nível de criptografia na rede, bem como a viabilidade da infiltração. Normalmente, não é muito simples a infiltração em uma rede privada com uma rígida criptografia, sendo necessário a obtenção do ID de algum usuário já integrante da comunidade, o que torna inviável o processo investigativo até que haja obtenção do acesso à rede.

Além disso, nos casos em que o crime for cometido na Deep Web, a infiltração torna-se mais difícil ainda, pois não basta meramente adentrar em um fórum ou site malicioso. É preciso adquirir o endereço de IP para que seja efetuado o

[33] PEREIRA, Flávio Cardoso. Agente Infiltrado Virtual (Lei n. 13.441/17): Primeiras impressões. **Revista do Ministério Público do Estado de Goiás**, v. 97, 2017. Disponível em: http://www.mp.go.gov.br/revista/pdfs_12/8-ArtigoFlavio_Layout%201.pdf. Acesso em: 28 set 2021.

devido rastreamento, o que não seria possível dentro da Dark Web pela modificação de IP realizado pela ferramenta TOR, devendo a autoridade policial identificar outros meios de prova ou atrair determinado usuário para fora da Deep Web.

Isto posto, o êxito da operação de infiltração no mundo digital depende de uma série de procedimentos a serem adotados pelo Ministério Público e delegado de polícia. Após a autorização judicial, deverá ser designado um agente policial técnico, dentro do quadro de agentes, com capacidade de atuação intensiva na rede mundial de computadores.[34] Por esse motivo, o conhecimento informático do agente a ser infiltrado deve ser levado em consideração na seleção efetuada pela autoridade policial.

3.2 Eficiência da infiltração policial nos crimes de caráter sexuais contra crianças e adolescentes

A Lei 13.441/2017 foi responsável por regular a infiltração policial nos meios virtuais, mas isso não significa dizer que as operações policiais virtualmente começaram a partir da referida lei. O Ministério Público em conjunto com a Polícia Federal já executou diversas operações anteriores a 2017 cuja medida consistia na infiltração do agente na rede virtual para a obtenção de informações e dados a serem utilizados na persecução penal. A principal dessas operações seria a Darknet realizada em 15 de outubro de 2014 e 22 de novembro de 2016.[35]

O embasamento legal utilizado nas operações constava na Lei 12.850/13, o qual continha a forma genérica da infiltração, o que abrangeria todas as outras modalidades, incluindo a digital. Nessa perspectiva, como referida lei possibilitava a adoção da infiltração nos crimes previstos em tratados internacionais cujo Brasil é signatário, foi utilizada a Convenção Internacional sobre os direitos das crianças de

---

[34] COSTA JÚNIOR, José Carlos Teixeira. Limites da Infiltração Policial na Internet e a Invasão de Dispositivo Informático: O advento da Lei 13.441/2017. Trabalho de Conclusão de Curso na Universidade Federal da Bahia. Salvador. 2018. Disponível em: https://repositorio.ufba.br/ri/bitstream/ri/26249/1/Jos%c3%a9%20Carlos%20Teixeira%20Csta%20J%c3%banior%20-%20Infiltra%c3%a7%c3%a3o%20policial%20na%20Internet%20e%20o%20crime%20do%20art.%20154-A.pdf. Acesso em: 28 set 2021.

[35] RODRIGUES, Felipe José Sousa; CARDOSO, Sarah de Araújo Mendes; MARWELL, Tatiana Eulálio Dantas Guedes. Utilização da infiltração virtual nas operações policiais para o combate aos crimes sexuais contra crianças e adolescentes. **Research, Society and Development**, v. 10, n. 4, p. e24710414152-e24710414152, 2021.

20 de novembro de 1989 para fundamentar diversas operações com policiais infiltrados na rede.

Uma das primeiras grandes atuações policiais na rede foi 2012 recebendo o nome operação de DyrtNet, o qual contava com o apoio do Ministério Público e da Interpol. Nela, foi identificado a existência de uma rede social fechada chamada Gigatribe, o qual continha inúmeros compartilhamentos de material pornográfico infanto-juvenil pelos suspeitos na condição de anônimos.[36] A dificuldade de o policial adentrar na rede era justificada pela sua rígida criptografia, sendo necessário a utilização de algum perfil já existente para que houvesse o acesso aos arquivos ilícitos.

Na referida operação, a Polícia Federal, utilizando-se da prisão de um dos usuários da Gigatribe na operação anterior chamada de Caverna do Dragão, fez uso do Nickname do infrator preso para se infiltrar na rede. Com isso, foram apreendidos diversos arquivos, contendo cenas de estupros de bebês, assassinato de crianças, abusos sexuais de menores, dentre outras.[37] Posteriormente a referida investigação, foram presas 32 pessoas, conforme o Balanço Final da Polícia Federal de Porto Alegre.[38] Nesse contexto, houve a êxito na deflagração da operação, sendo que a identificação de todos os usuários da rede contendo material ilícito somente foi possível em virtude da infiltração dos policiais de forma digital na Gigatribes.

Outra operação realizada pela Polícia Federal em 2014 e 2016 ficou conhecida como Darknet I e II. Nessa operação, a autoridade policial buscou infiltrar-se na área denominada como "submundo" da internet, a Deep Web, sendo uma tentativa de identificar os usuários que postavam conteúdo pornográfico infanto-juvenil. Como dito no capítulo anteriormente, o acesso a essa rede se dá pela ferramenta TOR, modificando constantemente o endereço de IP do usuário, o que

[36] RODRIGUES, Felipe José Sousa; CARDOSO, Sarah de Araújo Mendes; MARWELL, Tatiana Eulálio Dantas Guedes. Utilização da infiltração virtual nas operações policiais para o combate aos crimes sexuais contra crianças e adolescentes. **Research, Society and Development**, v. 10, n. 4, p. e24710414152-e24710414152, 2021.

[37] RODRIGUES, Felipe José Sousa; CARDOSO, Sarah de Araújo Mendes; MARWELL, Tatiana Eulálio Dantas Guedes. Utilização da infiltração virtual nas operações policiais para o combate aos crimes sexuais contra crianças e adolescentes. **Research, Society and Development**, v. 10, n. 4, p. e24710414152-e24710414152, 2021.

[38] SUPERINTENDÊNCIA DA POLÍCIA FEDERAL. Balanço Final da Operação DirtyNet. 2012. Disponível em: http://www.pf.gov.br/agencia/noticias/2012/junho/balanco-final-da-operacao-dirty-net. Acesso em: 28 set 2021.

dificultava o rastreio. Diante disso, a autoridade policial se encontrava impelida de averiguar autores dos conteúdos ilícitos contidos na Dark Web.

Para solucionar a questão do rastreio, a autoridade policial, com autorização judicial, criou um ambiente virtual controlado pelos agentes chamado de fórum Forpedo Brasil, idêntico aos demais fóruns contidos na Deep Web.[39] O acesso a esse fórum somente seria possível mediante o cadastro prévio que direcionava os usuários a um site localizado na Superface Web (internet de fácil acesso pelo sistema de busca), o que permitiria a identificação e rastreamento do endereço de IP.[40] Portanto, a operação em si utilizou-se de um artifício tecnológico para atrair os usuários ocultos na Dark Web para a área visível da internet, com a finalidade de desvendar a autoria delitiva.

Nota-se que a operação policial foi bem-sucedida, identificando materiais postados por indivíduos residentes no Brasil e no exterior, havendo o compartilhamento de dados com a Interpol. Na decisão judicial que fundamentou a condenação, os desembargadores consideraram que a criação do fórum não seria classificada como flagrante forjado, proibido no ordenamento jurídico, mas sim seria um flagrante esperado, uma vez que os delinquentes já estavam em posse do material ilícito e possuíam intenção de postar o conteúdo pornográfico infantil, bem como os policiais meramente esperaram a concretização do delito.[41]

Em suma, é possível verificar o êxito das operações efetuadas com a infiltração virtual, sendo essa um mecanismo indispensável à obtenção tanto da materialidade quanto da autoria delitiva. Nesse contexto, nos crimes virtuais, como há uma ocultação do endereço de IP, principalmente dos delitos praticados na Deep Web que usam a ferramenta do TOR, é indispensável a figura do agente infiltrado, a fim de atrair o suspeito para fora da interface oculta da internet.

---

[39] RODRIGUES, Felipe José Sousa; CARDOSO, Sarah de Araújo Mendes; MARWELL, Tatiana Eulálio Dantas Guedes. Utilização da infiltração virtual nas operações policiais para o combate aos crimes sexuais contra crianças e adolescentes. **Research, Society and Development**, v. 10, n. 4, p. e24710414152-e24710414152, 2021.

[40] Brasil. (2019). Acórdão. Recurso em Sentido Estrito n. 00131528920144036181 SP. 07 de janeiro de 2019. 11ª Turma do TRF da 3ª Região.

[41] Brasil. (2019). Acórdão. Recurso em Sentido Estrito n. 00131528920144036181 SP. 07 de janeiro de 2019. 11ª Turma do TRF da 3ª Região.

4 CONCLUSÃO

O mundo digital e a consequente proliferação dos delitos sexuais contra as crianças e adolescentes precisam ser amplamente combatidos pelo Estado. A criança muitas vezes utiliza-se da rede virtual sem o devido acompanhamento dos responsáveis, sendo alvo de manipulação por parte dos infratores. Não somente isso, como existe o compartilhamento de material pornográfico infanto-juvenil nos meios digitais, normalmente de acesso restrito, sendo que esses vídeos e fotos são originários de sequestro de crianças ou provenientes dos próprios responsáveis que vendem o conteúdo com a finalidade de obter vantagem econômica.

Como a vítima dos delitos são crianças, isto é, possuem o desenvolvimento mental ainda incompleto, dificilmente os atos sofridos são compartilhados com seus responsáveis ou com alguma autoridade policial. Naturalmente, o fato delituoso somente passa a ser externado quando o indivíduo atingiu uma certa maturidade. Portanto, a investigação do delito praticado contra a criança começa, na maioria dos casos, após um lapso temporal extenso entre o ato e a ciência pelo delegado de polícia.

Ademais, o compartilhamento do conteúdo sexual infantil é realizado pela área oculta na internet, onde os navegadores não alcançam, sendo conhecido como Deep Web. O usuário para acessar a referida rede deve utilizar um programa especial, tais como o TOR, que modificam constantemente o endereço de IP do usuário, dificultando o seu rastreamento. Desta feita, a investigação voltada a descoberta de eventual materialidade e autoria delitiva encontra-se amplamente dificultada em alguns casos de crimes cometidos na rede, seja pela rígida criptografia do site ou pela impossibilidade de rastreio do IP em virtude de aplicativos que o modifique.

Dito isso, o presente artigo buscou elucidar sobre a infiltração policial como forma de combate ao crime cometido na rede virtual. O policial, utilizando-se de um perfil falso na rede, trafega nos sites e fóruns contendo materiais pornográficos envolvendo crianças e adolescentes, com a finalidade de obter as provas de materialidade e autoria delitiva, podendo inclusive atuar no processo como

testemunha. O principal objetivo do agente infiltrado seria conseguir o endereço de IP do autor do fato delituoso, para efetuar o seu rastreamento.

Como esse meio de prova adentra na privacidade individual, a autuação do policial depende de autorização judicial, sendo necessário: o requerimento do Ministério Público ou representação do delegado de polícia; indícios mínimos de materialidade e autoria delitiva; demonstrar a impossibilidade de comprovação do fato delituoso por outros meios de prova; a capacidade de obter êxito na investigação com a infiltração policial.

Nesse contexto, restou amplamente demonstrado, nas operações policiais que adotaram a infiltração policial, tais como a Dyrtnet e a Darknet, a capacidade de identificação tanto da autoria quanto da materialidade delitiva. A realização de infiltração por meio de nicknames falso no local de compartilhamento de material ilícito sobre crianças e adolescentes permitiria a identificação dos usuários daquele site malicioso, sem necessitar quebrar a rígida criptografia. Portanto, a infiltração policial mostra-se como uma técnica eficaz na obtenção de provas para embasar a persecução penal.

Em suma, a realização de uma operação conjunta entre dos diferentes órgãos policiais, com a adoção de técnicas de infiltração, seria uma forma de salvaguardar diversas crianças que venham a ser vítima dos delitos em envencilha. O monitoramento policial na rede mundial de computadores, principalmente no âmbito da Deep Web, onde há a maior concentração de delitos, seria imprescindível na era digital moderna. As crianças, futura base da sociedade, devem ser amplamente protegidas contra a sexualização precoce, o que torna essencial a modernização das técnicas de atuação policial.

REFERÊNCIAS

ALMEIDA, Kesller Cristina Silva de. Infiltração policial no âmbito virtual como meio extraordinário de investigação criminal. Monografia apresentada à Universidade Federal do Paraná. Curitiba. 2019. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/68068/Monografia%20-%20Kesller%20Cristina%20Silva%20de%20Almeida%20%282019%29.pdf?sequence=1&isAllowed=y. Acesso em: 28 set 2021.

ÂNGELO, Luíza Alice Torres. Crimes cibernéticos: as limitações da resposta estatal a criminalidade informática. 2017. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/11418/1/LATA07062017.pdf. Acesso em: 28 set 2021.

BINI, Adriano Krul. **O agente infiltrado:** perspectivas para a investigação criminal na contemporaneidade. 2017. Dissertação de Mestrado da Instituto Superior de Ciências Policiais e Segurança Interna – ISCPSI. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/25429/1/DISSERTA%C3%87%C3%83O%20FINAL%20%20%20ap%C3%B3s%20j%C3%BAri.pdf. Acesso em: 28 set 2021.

BRASIL. Acórdão. Recurso em Sentido Estrito n. 00131528920144036181 SP. 07 de janeiro de 2019. 11ª Turma do TRF da 3ª Região.

BRASIL. Lei 8.069. Estatuto da Criança e Adolescente. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm#art240. Acesso em: 28 set 2021.

CARVALHO, Lucas Machado. A prática da Pedofilia e Crimes Sexuais: A aplicação da Lei em Crimes Virtuais. Monografia apresentada à Universidade Católica de Goiás. 2020. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/955/1/LUCAS%20MACHADO%20CARVALHO.pdf. Acesso em: 28 set 2021.

CAVALCANTE, Laylana Almeida de Carvalho. Ciberpedofilia: crimes sexuais contra crianças e adolescentes praticados através da internet. **Research, Society and Development**, v. 9, n. 2, p. 23, 2020.

Comitê Gestor da Internet do Brasil. Resumo executivo: pesquisa TIC kids online brasil 2019. Disponível em: https://cetic.br/media/docs/publicacoes/2/20201123093441/resumo_executivo_tic_kids_online_2019.pdf. Acesso em: 28 set 2021.

COSTA JÚNIOR, José Carlos Teixeira. Limites da Infiltração Policial na Internet e a Invasão de Dispositivo Informático: O advento da Lei 13.441/2017. Trabalho de Conclusão de Curso na Universidade Federal da Bahia. Salvador. 2018. Disponível em: https://repositorio.ufba.br/ri/bitstream/ri/26249/1/Jos%c3%a9%20Carlos%20Teixeira%20Csta%20J%c3%banior%20-%20Infiltra%c3%a7%c3%a3o%20policial%20na%20Internet%20e%20o%20crime%20do%20art.%20154-A.pdf. Acesso em: 28 set 2021.

DE MATTOS, Kennedy Josué Greca. Crimes praticados na dark web e a dificuldade de resposta estatal. 2020. Disponível em: https://www.unifor.br/documents/392178/3101527/Kennedy+Josue+Greca+de+Mattos.pdf/fbab6502-5e60-b2e1-8d57-1b29fd65ba05. Acesso em: 28 set 2021.

JOSÉ, Maria Jamile. **A infiltração policial como meio de investigação de prova nos delitos relacionados à criminalidade organizada**. 2010. Tese de Doutorado. Universidade de São Paulo. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-01122010-144008/publico/Infiltracao_policial_Maria_Jamile_Jose.pdf. Acesso em: 28 set 2021.

PEREIRA, Flávio Cardoso. Agente Infiltrado Virtual (Lei n. 13.441/17): Primeiras impressões. **Revista do Ministério Público do Estado de Goiás**, v. 97, 2017. Disponível em: http://www.mp.go.gov.br/revista/pdfs_12/8-ArtigoFlavio_Layout%201.pdf. Acesso em: 28 set 2021.

PIRES, Luiza Matias. A infiltração policial virtual nos crimes contra a dignidade sexual da criança e do adolescente: análise da infiltração sob a ótica da lei 13.441/17. **ISSN 1677-1281**, v. 36, n. 36, 2018.

RODRIGUES, Felipe José Sousa; CARDOSO, Sarah de Araújo Mendes; MARWELL, Tatiana Eulálio Dantas Guedes. Utilização da infiltração virtual nas operações policiais para o combate aos crimes sexuais contra crianças e adolescentes. **Research, Society and Development**, v. 10, n. 4, p. e24710414152-e24710414152, 2021.

SAFERNET BRASIl. Denúncias de pornografia infantil cresceram 33,45% em 2021, aponta a Safernet Brasil. 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil-cresceram-3345-em-2021-aponta-safernet-brasil. Acesso em: 28 set 2021.

SATO, Gustavo Worcki. A infiltração virtual de agentes e o combate à pedopornografia digital: estudo da lei 13.441/2017 e lei 13.964/2019. **J²-Jornal Jurídico**, v. 4, n. 1, p. 163-181, 2021.

SUPERINTENDÊNCIA DA POLÍCIA FEDERAL. Balanço Final da Operação DirtyNet. 2012. Disponível em: http://www.pf.gov.br/agencia/noticias/2012/junho/balanco-final-da-operacao-dirty-net. Acesso em: 28 set 2021.

TELES, Ketlhen Rayane Nunes de Sá. Crimes virtuais de pornografia infantojuvenil e pedofilia: um estudo sobre os fluxos de investigações. Centro Universitário FG. Guanambi. Bahia. 2021. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/13478/1/TCC%20II%20FINALIZADO%20KETLHEN%20RAYANE%20NUNES%20DE%20S%c3%81%20TELES.pdf. Acesso em 28 set 2021.

DOS ASPECTOS FUNDAMENTAIS ACERCA DA REGULAMENTAÇÃO DOS CRIMES CIBERNÉTICOS NO BRASIL

Samanta Bárbara Ribeiro do Nascimento[1]

RESUMO

O presente artigo científico trata-se de estudo acadêmico realizado sobre os aspectos fundamentais acerca da regulamentação dos crimes cibernéticos no Brasil. Como é cediço, verifica-se que os crimes virtuais estão em bastante evidência atualmente, pois é crescente a quantidade de usuários que acessam a internet, utilizando-se da tecnologia como ferramenta para obtenção de vantagens indevidas com objetivo de prejudicar terceiros. Diante da popularidade e acessibilidade do mundo da internet, indivíduos todos conectados vêm se tornando destaque de práticas criminosas no Brasil, em decorrência do aumento de condutas criminosas e o crescimento de denúncias de vítimas de crimes cibernéticos, fatos ocasionados devido à facilidade de acesso à internet, bem como a fragilidade do ambiente virtual sem um mínimo de segurança de informações. Ademais disso, destaca-se ainda que a problemática está relacionada com a fragilidade na regulamentação e na dificuldade de identificação dos autores de tais delitos tendo em vista ser um ambiente obscuro e coberto de anonimatos. Por tal motivo, diante falta de previsão legal na reprovabilidade dos crimes em destaque, bem como na dificuldade de identificação, torna-se um fator preocupante perante a sociedade, requerendo de imediato surgimento de legislação específica. Desse modo, será abordado no presente artigo, os aspectos cruciais acerca da ideia de crimes virtuais, tecer considerações sobre a evolução histórica dos delitos cibernéticos no Brasil bem como identificar a existência de regulamentação do crime no Brasil e verificar os anseios e as dificuldades existentes no âmbito investigatório criminal sobre a identificação da autoria delitiva. Para tanto, como método de abordagem que proporcionará reflexão do tema, utilizar-se-ão textos concisos e informativos, como também, os métodos dedutivos e indutivos, utilizando como método de procedimento e como técnicas de pesquisa, a documentação direta, ou seja, Constituição Federal, Código Penal, Código de Processo Penal e jurisprudências, e indireta, as revisões bibliográficas, websites, artigos, e documentários, sobre o tema em estudo.

[1] Bacharel em Direito, Centro Universitário de Brasília - UniCEUB, Instituto CEUB de Pesquisa e Desenvolvimento - ICPD, SEPN 707/907, Campus UNICEUB, Cep nº 70.790-075, Brasília/DF, e-mail: samanta_bnascimento@hotmail.com.

Palavras-Chave: Crimes Cibernéticos. Regulamentação Específica. Punibilidade.

ABSTRACT

This scientific article is an academic study carried out on the fundamental aspects of the religion of cybercrime in Brazil. As it is old, it appears that cybercrime is in evidence nowadays, as the number of users on social networks is increasing, using the internet as a tool to obtain illicit advantages and harm third parties. Given the generation and accessibility of the internet world, not all connected, it has become a highlight of criminal practices in Brazil, in view of the increase in illegal conduct and the growth of complaints from victims of virtual crimes, facts caused due to the ease of access internet, as well as the fragility of the virtual environment, without a minimum of information security. In addition, it is also highlighted that the problem is related to the weakness of reception and the difficulty of identifying the perpetrators of such crimes, considering that it is an obscure environment covered with anonymity. For this reason, given the lack of legal provision in the reprobability of the highlighted crimes, as well as in the identification, it becomes a worrying factor for society, requiring the immediate creation of specific legislation. Thus, this article will address the crucial aspects of the design of virtual crimes, make considerations about the historical evolution of cyber crimes in Brazil, as well as identify the existence of crime in Brazil and verify how difficulties exist in the criminal investigation context on the identification of criminal authorship. Therefore, as a method of approach that will provide reflection on the topic, concise and informative texts will be used, as well as deductive and inductive methods, using as a method of procedure and as research techniques, the direct, that is, Federal Constitution, Penal Code, Code of Criminal Procedure and jurisprudence, and indirect, such as bibliographical reviews, websites, articles, and documentaries, on the subject under study.

Keywords: Cyber Crimes. Specific Regulation. Punishment.

1 INTRODUÇÃO

O presente trabalho é fruto de um recorte feito a partir de estudos realizados em documentações diretas e indiretas, na qual abordará de forma precípua os aspectos fundamentais acerca da regulamentação dos crimes cibernéticos no Brasil, destacando primordialmente os aspectos principais acerca da conceituação dos crimes virtuais, a evolução histórica dos delitos cibernéticos no Brasil, bem como relatar a existência de previsão legal do crime em estudo e as dificuldades vividas no âmbito investigatório sobre a identificação dos autores do delito.

Desde o início dos tempos, o surgimento do mundo digital trouxe grandes expectativas de evolução e fascínio por ser um ambiente novo e obscuro para a sociedade. Desta feita, com o crescimento da popularidade do uso da internet em

diversos âmbitos e atividades, surgiu também a preocupação com a segurança das informações compartilhadas de forma virtual pelos usuários.

Como é notório, os crimes virtuais estão intimamente ligados ao âmbito da internet propriamente dito, por intermédio dos meios de interação social como sites de navegação, aplicativos *WhatsApp, Instagram, Facebook*, e demais ambientes de acesso ao sistema virtual, estes que estão sujeitos a prática de condutas criminosas, onde estes em grande parte estão de frente ao anonimato.

Assim, surge para o Estado o dever de fiscalização e de reprovabilidade de tais condutas criminosas mediante aplicação medidas e de leis mais severas. Verifica-se que a legislação brasileira não trata com grande rigor as práticas de crimes virtuais, tendo em vista que algumas leis que estão em vigência prever tão somente penas brandas que possuem pena máxima três anos de detenção, com previsão de regime inicial aberto, como é o caso da famosa Lei Carolina Dieckmann[2], que na maioria das vezes, tais penas são convertidas em prestação de serviços a comunidade ou até mesmo pagamento de cestas básicas.

Diante do surgimento da ocorrência de tais condutas criminosas percebe-se que a obtenção das provas de autoria no meio dos crimes virtuais é incerta, às vezes impossível, tendo em vista a dificuldade na realização do procedimento investigatório devido à complexidade na apuração de informações precisas do crime. Portanto, é preciso que seja preservado o máximo possível à validade da prova, para que seja considerada idônea, para isso é necessário obter o endereço do IP, este que é a identidade virtual do provedor que houve a prática criminosa.

Por outro lado, destaca-se que antes da ocorrência da pandemia, ou seja, no ano de 2019, o Brasil já ocupava a terceira colocação no *ranking* dos países que mais foram vítimas de ataques cibernéticos conforme relatório global divulgado pela *Symantec*. Na mesma linha, já nos meses de janeiro a setembro do ano de 2020, o Brasil chegou a sofrer mais de 3,4 bilhões de tentativas de ataques de crimes

[2] BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. **Disponível em:** < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>**. Acesso em: 05 de set. de 2021.**

virtuais, conforme dados levantados pelas empresas *Fortinet Threat Intelligence Insider Latin America* [3].

Para tanto, como método de abordagem, foram utilizados métodos dedutivos e indutivos. Por sua vez, como método de procedimento e como técnicas de pesquisa foram utilizadas documentações diretas, ou seja, leis e doutrinas sobre o tema de crimes cibernéticos, e indireta, as pesquisas bibliográficas, artigos, e documentários, sobre o tema em estudo.

Assim, para melhor desenvolver o presente artigo, após o capítulo introdutório, tem-se que no segundo capítulo será demonstrado resumidamente a evolução histórica dos crimes virtuais, fazendo referência à evolução da internet, desde seu surgimento até a sua propagação na sociedade, destacando os conceitos históricos, as análises das ocorrências dos casos de crimes cibernéticos no Brasil.

Já no terceiro capítulo, serão analisados os aspectos fundamentais acerca do conceito inicial dos crimes cibernéticos, conforme doutrinas e artigos científicos sobre o tema, criando uma conexão com os capítulos seguintes, onde serão objetos de discussão sobre os crimes previstos no âmbito da internet.

De outro modo, no quarto capítulo, tratará sobre as regulamentações previstas acerca das espécies dos crimes cibernéticos vigentes no Brasil, e como a legislação brasileira lida com a aplicabilidade destes delitos. Enquanto o quinto capítulo trata da conclusão do presente artigo.

2 DA EVOLUÇÃO HISTÓRICA DOS CRIMES VIRTUAIS

Inicialmente, importante destacar, que a internet, conhecida também como "rede mundial de computadores", sobreveio durante a guerra fria, em decorrência de uma disputa entre os países dos Estados Unidos da América e a União Soviética,

[3] AC CERTIFICAMINAS. Crypto ID. **Crescimento de crimes cibernéticos na pandemia**: como não ser uma vítima. Disponível em: <https://cryptoid.com.br/identidade-digital-destaques/crescimento-de-crimes-ciberneticos-na-pandemia-como-nao-ser-uma-vitima/>. Acesso em: 08 de set. de 2021.

onde se destacavam a eficácia e a necessidade da utilização dos meios de comunicação obter garantir vantagens e até mesmo a vitória em disputas guerras[4].

De tal modo, observa-se que a internet surgiu como ferramenta de proteção de computadores e das informações do Governo Norte Americano. Ademais, a utilização e exploração da internet era restrita ao ambiente militar e universitário, ocasião em que somente no final da década de 70, e início da década de 80, a internet passou a ser utilizada para o comércio e disponibilizada para a população, devido o surgimento da Rede Minitel na França.

A cerca da evolução histórica dos crimes virtuais, verifica-se que antes de ser utilizada como instrumento para a prática de crime, a tecnologia era considerada moderna, no decorrer dos anos, foi objeto de rejeições e sabotagem pela sociedade, geralmente ocasionadas pelos indivíduos de baixo desenvolvimento educacional, que trabalhavam no período da Revolução Industrial de forma braçal[5].

Verifica-se que a ocorrência dos primeiros crimes virtuais veio na tentativa de rejeições e sabotagem dos sistemas de tecnologias existentes a época, devido à expansão da internet e o crescimento dos usuários, ocasionando grandes discussões acerca da segurança dos dados e informação, como também pela oportunidade de ocorrência de delitos[6].

Ademais, importante destacar que os primeiros crimes informáticos ocorreram no ano de 1960, nos Estados Unidos, a época, surgiram nos meios de comunicação norte-americanos, nos casos de uso de computadores para cometimento de delitos. Somente na década seguinte, foram iniciados estudos sistemáticos e científicos sobre o tema. Já no ano de 1980, as práticas criminosas se intensificaram, envolvendo condutas criminosas de pornografia infantil, de

[4] NASCIMENTO, Natália Lucas do. **Crimes cibernéticos**. Fundação Educacional do Município de Assis – FEMA. 2016. Disponível em: < https://cepein.femanet.com.br/BDigital/arqTccs/1311401614.pdf>. Acesso em 09 de set. 2021.

[5] JESUS, Damásio de. MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo. Editora Saraiva, 2016, p. 22.

[6] ROCHA, A. A. **Cibercriminalidade**: os crimes cibernéticos e os limites da liberdade de expressão na internet. Faculdade de Ensino Superior e Formação Integral. Curso de Direito. São Paulo, 2017. Disponível em: <https://www.faef.br/userfiles/files/23%20-%20CIBERCRIMINALIDADE%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20NA%20INTERNET.pdf> Acesso em 8 de set. 2021.

manipulação de dados bancários, abusos de telecomunicações e pirataria de programas de computadores, dentre outros[7].

Portanto, a ideia de crimes informáticos somente veio ganhar destaque de forma mais específica décadas após a Revolução Industrial. De acordo com os doutrinadores Damásio de Jesus e José Antônio Milagre, existem divergências sobre o surgimento do primeiro crime virtual propriamente dito durante a história, consistente entre dois fatos, acontecidos em duas universidades norte americanas, uma ocorrida no ano de 1964 e outra no ano de 1978, onde estudantes invadiram o sistema de segurança de dados computadorizados das universidades[8].

Importante destacar, que no Brasil a internet surgiu no ano de 1988, devido o relacionamento entre algumas universidades do Brasil com as instituições dos Estados Unidos, sendo que com passados alguns anos, foram se aprimorando, bem como disponibilizado para a população em geral.[9]

O Brasil passou a integrar o mundo globalizado e ter sua capacidade estrutural de adequar-se ao uso da tecnologia, durante os anos de 1980 e 1990.[10] Por sua vez, a revolução digital surgiu como um grande desenvolvimento para a sociedade visto que houve uma facilidade para o desenvolvimento de serviços e da rotina dos indivíduos na sociedade.

Deste modo, tem-se que os crimes virtuais estão intimamente ligados ao âmbito da internet, por intermédio dos meios de interação social, como sites de navegação, aplicativos *WhatsApp, Instagram, Facebook*, e demais ambientes de acesso ao sistema virtual, estes que estão sujeitos a prática de condutas criminosas. Deste modo, a informatização por meio digital, por sua vez, não tinha regulamentação sobre as limitações de uso no decorrer do tempo, porém, era

---

[7] BRASIL. **Conheça a evolução dos crimes cibernéticos**. Câmara dos Deputados. Publicado em 23/08/2006. Disponível em: <https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos/>. Acesso em: 8 de set. 2021.

[8] JESUS, Damásio de. MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo. Editora Saraiva, 2016, p. 23.

[9] NASCIMENTO, Natália Lucas do. **Crimes cibernéticos**. Fundação Educacional do Município de Assis – FEMA. 2016. Disponível em: < https://cepein.femanet.com.br/BDigital/arqTccs/1311401614.pdf>. Acesso em 09 de set. 2021.

[10] FIORILLO, C. A. P. CONTE, C. P. **Crimes no meio ambiente digital**. 2ª Edição. São Paulo: Editora Saraiva, 2016, p. 24.

previsto somente as normas de condutas já existentes atualmente referentes aos crimes e direitos, comumente praticados contra terceiros[11].

3 DO CONCEITO DOS CRIMES CIBERNÉTICOS

Como é cediço, diante do surgimento das atividades ilícitas oriundas no ambiente virtual, e por tais crimes serem considerados um tema atual, devido às condutas praticadas mediante utilização de computadores e *smartphones*, por intermédio da internet, estes ainda não possuem uma nomenclatura específica e definitiva.

Desse modo, tem-se que as denominações são variadas, podendo ser conhecidas como crimes cibernéticos, cibercrimes, crimes informáticos, crimes virtuais, dentre outros. Portanto, todas essas nomenclaturas referem-se ao mesmo tipo penal, ou seja, crimes que se utilizam de um computador ou *smartphones* com acesso a internet para praticar delitos. Assim, podemos classificar os crimes cibernéticos como sendo puros e impuros.

Assim, verifica-se que o crime cibernético puro está relacionado à ocorrência da conduta do agente em atacar o sistema informático de um terceiro, ou seja, um sistema um *software, hardware*, sistema e meios de armazenamento de dados.

Por sua vez, os crimes cibernéticos impuros, estão relacionados à conduta do agente que se utiliza da internet como meio executório para prática de um crime tipificado no Código Penal, como por exemplo, a incidência do crime de divulgação de fotografias pornográficas de crianças e adolescentes, tipificada no artigo 241, do Estatuto da Criança e do Adolescente.

Com o surgimento do mundo digital, trouxe grandes expectativas de evolução, por ser um ambiente novo e obscuro para a sociedade. Desta feita, com o crescimento da popularidade do uso da internet em diversos âmbitos e atividades, surgiu também a preocupação com a segurança das informações compartilhadas de forma virtual pelos usuários.

---

[11] ASSUNÇÃO, A. A. S. **Crimes virtuais.** UniEvangélica. Curso de Direito. Anápolis, 2018. Disponível em: <http://repositorio.aee.edu.br/bitstream/aee/538/1/Monografia%20-%20Ana%20Paula%20Souza.pdf>. Acesso em: 8 de set. de 2021.

De tal modo, a conceituação do termo cibercrime teve evidência no final da década de 90, em uma reunião realizada pelo G8, que tinha como objetivo à discussão do combate a práticas ilícitas no âmbito da internet, buscando uma solução para prevenir e punir tais condutas. Ocasião em que o termo passou a ser utilizado para referir-se aos crimes penais praticados virtualmente.

Do mesmo modo, os termos de crimes cibernéticos, conhecidos também como crimes virtuais, de acordo com os ensinamentos dos doutrinadores Damásio de Jesus e Antônio Milagre[12], consiste nos fatos típicos e antijurídicos cometidos por meio dá ou contra a tecnologia da informação, ou seja, um ato típico e antijurídico, cometido através da informática em geral.

Entretanto, a progressiva mutação tecnológica dificulta o combate a esses crimes, que estão em constante alinhamento com as novas tecnologias. Assim, com o uso incontido e indiscriminado da internet, alguns indivíduos com conhecimento em informática passaram a se aprimorar e utilizar esses conhecimentos para roubar informações criptografadas, como já havia sendo feito há muito tempo, para obter proveito econômico ou ainda, por mera diversão.

De acordo com Adriano Aparecido Rocha, o crime cibernético refere-se às condutas ilícitas realizadas por algum tipo de dispositivo tecnológico, por entender-se que as realizações das condutas são dadas em um ambiente virtual[13], como também aponta que os crimes cibernéticos são divididos como crimes próprios e crimes impróprios.

Por outro lado, com relação aos crimes próprios, tem-se que as condutas antijurídicas e culpáveis, onde o objetivo central é de prejudicar um sistema ou violar dados de segurança, e, nos crimes impróprios, encontram-se as conditas comuns, também antijurídicas e culpáveis, porém também consideradas típicas, que podem ter a sua ocorrência fora do ambiente virtual.

---

[12] JESUS, Damásio de. MILAGRE, José Antônio**. Manual de crimes informáticos**. São Paulo. Editora Saraiva, 2016, p. 9.

[13] ROCHA, A. A. **Cibercriminalidade: os crimes cibernéticos e os limites da liberdade de expressão na internet**. Faculdade de Ensino Superior e Formação Integral. Curso de Direito. São Paulo, 2017. Disponível em: <https://www.faef.br/userfiles/files/23%20-%20CIBERCRIMINALIDADE%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20NA%20INTERNET.pdf> Acesso em: 8 de set. 2021.

De acordo com Assunção, os crimes impróprios são os mais comuns de ocorrerem, que envolvem a liberdade de expressão junto ao discurso de ódio, porém devido à liberdade de expressão ser um direito garantido por lei a mesma não pode transgredir os limites que se iniciam aos direitos de terceiros, contra a sua imagem, privacidade, honra, intimidade etc.[14].

4 DA REGULAMENTAÇÃO PREVISTA AS ESPÉCIES DOS CRIMES CIBERNÉTICOS

A internet é um ambiente volátil, onde a prática de atos cometidos por intermédio de computadores e *smartphones*, não podem ser isentos de responsabilidade criminal, caso ocorram condutas que se encontra em desacordo com a legislação. Os crimes virtuais são aqueles praticados por intermédio da utilização de internet, onde as vítimas podem ser qualquer indivíduo da sociedade, como também grandes empresas, órgãos públicos e organizações.

Ademais, por ser um meio eficiente, os agentes possuem uma facilidade na efetividade da prática criminosa. Como é cediço, existem inúmeros delitos praticados corriqueiramente no ambiente virtual. Nesse sentido, pretende-se discorrer sobre alguns crimes existentes e os mais recorrentes na esfera criminal.

De acordo com o Código Penal Brasileiro, em seu artigo 1º, estabelece que não haja crime sem lei anterior que o defina, não há pena sem prévia cominação legal, de forma que os crimes cibernéticos só passaram a receber a devida atenção após a criação e adequação ao ordenamento jurídico brasileiro, uma legislação específica, prevendo a reprovabilidade das condutas criminosas no ambiente virtual.

Por outro lado, com relação à criação da legislação penal específica acerca dos crimes virtuais, Ramos destaca que a Convenção sobre o Cibercrime não dita regras para sua criação, mas orienta, deixando a critério de cada país, criar sua própria legislação específica. Diante disso, o Estado, pode estabelecer a criação de suas leis, de acordo com suas exigências e particularidades, no que se refere ao

[14] ASSUNÇÃO, A. A. S. **Crimes virtuais.** UniEvangélica. Curso de Direito. Anápolis, 2018. Disponível em: <http://repositorio.aee.edu.br/bitstream/aee/538/1/Monografia%20-%20Ana%20Paula%20Souza.pdf>. Acesso em: 10 set. 2021.

ordenamento jurídico dos crimes cibernéticos, visando à identificação dos autores e a devida punição aos criminosos[15].

Por outro lado, destaca-se o crime de furto eletrônico, ou seja, referente às fraudes bancárias, onde se encontra prevista no artigo 155, §§3º e 4º, inciso II, do Código Penal, que fala que subtrair, para si ou para outrem, coisa alheia móvel, onde se equipara como coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico, com a utilização de meio de abuso de confiança, ou mediante fraude, escalada ou destreza, para obtenção da vantagem ilícita.

Do mesmo modo, tem-se o crime de estelionato digital, que tem com o objetivo principal, de enganar as vítimas, os agentes deste delito, utiliza-se de aspectos de vulnerabilidade, explorando as emoções das vítimas. Deste modo, tudo se inicia com uma página *fake* demonstrando ser uma empresa que oferece grandes oportunidades à vítima em troca de repasse de dinheiro. Os criminosos, após obterem êxito no recebimento da quantia, simplesmente somem, na maioria das vezes sem deixar quaisquer rastros. O crime de estelionato digital está previsto no artigo 171, do Código Penal, que diz que 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, incorre no crime de estelionato.

Ademais, como exemplo também temos o crime de invasão de dispositivo informático e furto de dados, previsto no artigo 154-A, do Código Penal, onde prever que invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita, comete o referido crime, com pena de reclusão, de um a quatro anos, ou aplicação de multa.

Do mesmo modo, temos o crime de falsificação e supressão de dados, delitos estes previstos nos artigos 297, 298, 299, 313-A, 313-B, todos, do Código Penal, onde descreve que, respectivamente, o agente que pratica a conduta de falsificar, no todo ou em parte, documento público, ou alterar documento público verdadeiro, ou

[15] RAMOS, E. D. **Crimes cibernéticos**: análise evolutiva e Legislação penal brasileira. Curso de Direito da Universidade Federal do Rio de Janeiro. 2017. Disponível em: < https://pantheon.ufrj.br/bitstream/11422/6911/1/EDRamos.pdf>. Acesso em: 11 de set. 2021.

falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro, ou omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante, ainda, se inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano, ou modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente, comete crime de falsificação e supressão de dados.

Por outro lado, temos a previsão dos crimes praticados contra crianças e adolescentes, que consiste no armazenamento, produção, troca, publicação de vídeos e imagens contendo pornografia infanto-juvenil, tais condutas tipificadas nos artigos 241 e 241-A, ambos, do Estatuto da Criança e do Adolescente, onde vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, ou em oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, incide nas penas previstas no presente delito.

No mesmo sentido, é o delito de assédio e aliciamento de crianças, descritos nos artigo 241-D, do Estatuto da Criança e do Adolescente, que prever que a conduta de aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso, responde pelo presente crime, com pena de reclusão, de um a três anos, e aplicação de multa.

Por outro lado, verifica-se a incidência nos crimes cibernéticos, o crime de ameaça, tipificado no artigo 147, do Código Penal, que consiste no ato de ameaçar alguém, através de palavras, gestos ou outros meios de lhe causar mal injusto e grave. A pena para esse crime pode variar de um a seis meses de prisão além do pagamento de multa. A ameaça no crime virtual é propagada mediante utilização dos

meios sociais, ou por mensagens via aplicativos de mensagens, fazendo com que o agente, incida nas penas do referido artigo.

No âmbito dos crimes cibernéticos, tem-se o crime de Cyberbullying, um dos mais corriqueiros dentro da internet, onde se refere à criação de publicações de perfis *fakes*, veiculando ofensas em blogs e comunidades virtuais, assim, tal pratica incide nas penas previstas nos artigos 138, 139, 140, todos, do Código Penal, onde relata que caluniar alguém, imputando-lhe falsamente fato definido como crime, ou difamar alguém, imputando-lhe fato ofensivo à sua reputação, ou injuriar alguém, ofendendo-lhe a dignidade ou o decoro, no ambiente virtual, impõe-se as penas descritas nos tipos penais.

Tem-se previsto também o crime incitação e apologia a prática de crime, tais tipos previstos nos artigos 286 e 287, ambos, do Código de Processo Penal, que prever que a conduta de incitar, publicamente, a prática de crime, ou fazer, publicamente, apologia de fato criminoso ou de autor de crime, incorre nas penas do tipo penal.

Pois bem, diante do crescimento de números de delitos virtuais e a grande repercussão na sociedade, decidiu o legislador a criar normas legais que objetivam a reprovabilidade de tais condutas criminosas. Nesse sentido, temos como exemplo a Lei dos Crimes Cibernéticos (Lei nº 12.737/12), ou mais conhecida como Lei Carolina Dieckmann.

A criação da Lei Carolina Dieckmann, foi considerada um marco histórico no ordenamento jurídico brasileiro como instrumento de combate aos crimes cibernéticos. Essa lei objetiva tipificar condutas altamente reprováveis, como é o caso do crime de invasão de computadores, roubo de senhas, violação de dados dos usuários e divulgação de informações privadas.

Diante disso, já era cogitada a criação da referida norma, diante do crescimento dos crimes virtuais, diante dos golpes e roubos de senhas por intermédio da internet, por sua vez, antes da publicação da lei, a mesma só ganhou notoriedade diante da repercussão do caso da modelo e atriz Carolina Dieckmann, onde teve seu computador invadido por criminosos e teve seus arquivos pessoais subtraídos,

posteriormente publicado mais de 36 fotos íntimas pelas redes sociais, que rapidamente se espalharam pela internet[16].

Assim, no decorre dos anos, o ordenamento jurídico brasileiro teve que atualizar suas normas, diante da ocorrência de novos casos de crimes virtuais. Por sua vez, o Código Penal brasileiro, teve que ser readaptado, com uma nova alteração, teve em seu texto o acréscimo dos artigos 154-A e 154- B, onde prever os crimes referentes as liberdades individuais, no que se refere à inviolabilidade dos segredos.

Nesse sentido, conforme já mencionado anteriormente, o artigo 154-A, o dispositivo exige a necessidade de que o mecanismo de segurança desse aparelho seja violado indevidamente, definindo, portanto, como fato atípico se caso não subsista o mecanismo de segurança[17]. Deste modo, é o que prever o texto do artigo 154-A, onde:

> 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.

Por outro lado, o artigo154-B, do Código Penal, prevê que:

> 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.

Entretanto, observa-se que a conduta de invasão de dispositivo informático, tem previsão de punição de pena de prisão de três meses a um ano ou aplicação de multa. Ademais, verifica-se que as condutas mais prováveis estão relacionadas na obtenção, pela invasão, conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, tendo em vista a pena ser de seis meses a dois anos de prisão, além da possibilidade de aplicação de pena de multa. Assim, diante de todos os exemplos de normas legais, teve como finalidade

---

[16] VITORIANO, Larissa. **A lei tipifica crimes virtuais e altera artigos do Código Penal**. Disponível em: <https://cpjur.com.br/lei-carolina-dieckmann/>. Acesso em: 15 de set. de 2021.

[17] QUINTINO, Eudes. **A nova lei Carolina Dieckmann**. JusBrasil. Disponível em: < https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann?>. Acesso em: 16 de set. 2021.

promover discussões acerca das condutas previstas nos crimes cibernéticos o ordenamento jurídico brasileiro.

5 CONCLUSÃO

O presente artigo científico buscou trazer elementos de discussão referente à aos aspectos fundamentais acerca da regulamentação dos crimes cibernéticos no Brasil, tomando-se como paradigma, o aumento dos casos de crimes virtuais, as dificuldades do reconhecimento da autoria delitiva, bem como a existência de previsão regulamentar específica, trazendo o crescimento dos estudos jurídicos atuais sobre o tema, assim aquecendo grandes debates jurídicos.

Verificou-se no decorrer deste artigo, que a internet é um ambiente volátil, onde a prática de atos cometidos por intermédio de computadores e *smartphones*, não podem ser isentos de responsabilidade criminal. Os crimes virtuais são aqueles praticados por intermédio da utilização de internet, onde as vítimas podem ser qualquer indivíduo da sociedade, como também grandes empresas, órgãos públicos e organizações.

Do mesmo modo, por ser um meio eficiente, os agentes possuem uma facilidade na efetividade da prática criminosa. Como é cediço, existem inúmeros delitos praticados corriqueiramente no ambiente virtual. Nesse sentido, a superexposição indevida no mundo virtual vem se tornando um problema cada vez mais comum, especialmente entre crianças e adolescentes que acessam os aplicativos de redes sociais. Por sua vez, tais hábitos podem trazer consequências bastante negativas.

Verificou-se que as vítimas dos crimes virtuais, são variadas, devido à superexposição ocasionada na internet, onde surgem e publicam acontecimentos de suas vidas, sendo submetidas ao estado de vulnerabilidade nas ações de criminosos no ambiente da internet, os quais praticam diversos e variados tipos de crimes, todos relacionados às pessoas, divulgação de segredos e violação de informações, cyberbullying, injúria e difamação, às transações comerciais mediante links falsos, clonagem de cartão de crédito, invasão por vírus em computadores, e crimes contra o patrimônio. Assim, resta-se clara a importância da atuação conjunta entre Estado e

sociedade a com objetivo de buscar solucionar e reduzir os riscos da ocorrência dos crimes cibernéticos.

Ademais, importante ainda destacar, que a grande incidência dos crimes cibernéticos perante as empresas é decorrente de práticas de crimes com a utilização de softwares, como é o caso dos cookies, spammings, spyware, hoaxes, backdoors, sniffer, cavalo de troia, worm e vírus.

Portanto, dito isto, embora a livre manifestação de pensamento seja assegurada pela Constituição Federal, há determinadas situações, como nos casos em que se fere a dignidade do indivíduo, em que a liberdade de expressão conflita com outros direitos fundamentais tão importantes quanto, por esse motivo, ela não pode ser absoluta.

Por fim, em razão da imensurável grandeza do mundo virtual, há muito que se explorar a respeito de como a superexposição na internet tem se tornado cada vez mais prejudicial para a geração atual, pois esse problema coloca em risco a segurança e a privacidade das pessoas.

Além disso, é importante também ressaltar, que as leis se tornem cada vez mais efetiva e rigorosa para impedir a prática de tais delitos, e que aquele criminoso irresponsável não venha a expor a vida de terceiros e não tragam prejuízos, em via de consequência, não saiam impunes e que tais crimes virtuais possam ser de fato reprováveis.

Todavia, atualmente existem poucas legislações que tipificam especificamente as condutas praticadas no âmbito virtual, o que, de fato, dificulta a punição dos criminosos, portanto faz-se necessário à criação de regulamentações específicas para o combate aos crimes virtuais, bem como que haja proteção na segurança das informações dos dados dos usuários de redes sociais.

REFERÊNCIAS

AC CERTIFICAMINAS. Crypto ID. **Crescimento de crimes cibernéticos na pandemia**: como não ser uma vítima. Disponível em: <https://cryptoid.com.br/identidade-digital-destaques/crescimento-de-crimes-ciberneticos-na-pandemia-como-nao-ser-uma-vitima/>. Acesso em: 08 de set. 2021.

ASSUNÇÃO, A. A. S. **Crimes virtuais.** UniEvangélica. Curso de Direito. Anápolis, 2018. Disponível em: <http://repositorio.aee.edu.br/bitstream/aee/538/1/Monografia%20-%20Ana%20Paula%20Souza.pdf>. Acesso em: 08 de set. 2021.

BRASIL. **Conheça a evolução dos crimes cibernéticos**. Câmara dos Deputados. Publicado em 23/08/2006. Disponível em: <https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos/>. Acesso em: 08 de set. 2021.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. **Disponível em: <** http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm**>. Acesso em: 05 de set. 2021.**

FIORILLO, C. A. P. CONTE, C. P. **Crimes no meio ambiente digital**. 2ª ed. São Paulo: Editora Saraiva, 2016. Página 24.

JESUS, Damásio de. MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo. Editora Saraiva, 2016.

MAIA, T. S. F. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro**. Universidade Federal do Ceará. Faculdade de Direito, Curso de Direito, Fortaleza, 2017. Disponível em: < http://www.repositorio.ufc.br/bitstream/riufc/31996/1/2017_tcc_tsfmaia.pdf>. Acesso em: 10 de set. 2021.

NASCIMENTO, Natália Lucas do. **Crimes cibernéticos**. Fundação Educacional do Município de Assis – FEMA. 2016. Disponível em: < https://cepein.femanet.com.br/BDigital/arqTccs/1311401614.pdf>. Acesso em: 09 de set. 2021.

QUINTINO, Eudes. **A nova lei Carolina Dieckmann**. JusBrasil. Disponível em: < https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann?>. Acesso em: 16 de set. 2021.

RAMOS, E. D. **Crimes cibernéticos**: análise evolutiva e legislação penal brasileira. Curso de Direito da Universidade Federal do Rio de Janeiro. 2017. Disponível em: < https://pantheon.ufrj.br/bitstream/11422/6911/1/EDRamos.pdf>. Acesso em: 11 de set. 2021.

ROCHA, A. A. **Cibercriminalidade:** os crimes cibernéticos e os limites da liberdade de expressão na internet. Faculdade de Ensino Superior e Formação Integral. Curso de Direito. São Paulo, 2017. Disponível em: <https://www.faef.br/userfiles/files/23%20-%20CIBERCRIMINALIDADE%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20NA%20INTERNET.pdf> Acesso em: 8 de set. 2021.

SANTOS, Nathalia Maria de Oliveira. **O limite das exposições nas redes sociais e o direito à liberdade de expressão:** um estudo sobre os efeitos negativos da superexposição das pessoas nas redes sociais e seus impactos no ordenamento jurídico. Fundação Educacional do Município de Assis – FEMA. São Paulo. 2020. Disponível em: < https://cepein.femanet.com.br/BDigital/arqTccs/1711401617.pdf>. Acesso em: 15 de set. 2021.

VITORIANO, Larissa. **A lei tipifica crimes virtuais e altera artigos do Código Penal**. Disponível em: <https://cpjur.com.br/lei-carolina-dieckmann/>. Acesso em: 15 de set. 2021.