BRASÍLIA 2020

ISBN 978-65-87823-26-3

CRIMES DIGITAIS

Coordenação:

LILIAN ROSE LEMOS ROCHA
PAULO BINICHESKI
DAVI BELTRÃO DE ROSSITER CORRÊA
VIVIANE DE MOURA FRAGOSO
ISRAEL ROCHA LIMA MENDONÇA FILHO
JOAO VICTOR ORLANDI

CEUB

ICPD Instituto CEUB de Pesquisa e Desenvolvimento

Coordenação
Lilian Rose Lemos Rocha
Paulo Binicheski
Davi Beltrão de Rossiter Corrêa
Viviane de Moura Fragoso
Israel Rocha Lima Mendonça Filho
Joao Victor Orlandi

CADERNO DE PÓS-GRADUAÇÃO EM DIREITO

CRIMES DIGITAIS

Brasília
2020

CEUB

ICPD Instituto CEUB de Pesquisa e Desenvolvimento

CENTRO UNIVERSITÁRIO DE BRASÍLIA - UniCEUB
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

Projeto gráfico
UniCEUB/ACC
André Luís César Ramos

Diagramação
Biblioteca Reitor João Herculino

Capa
UniCEUB

Documento disponível no link
https://www.repositorio.uniceub.br

Dados Internacionais de Catalogação na Publicação (CIP)

Caderno de pós-graduação em direito: crimes digitais / coordenadores, Lilian Rose Lemos Rocha et al. – Brasília: UniCEUB: ICPD, 2020.

381 p.

ISBN 978-65-87823-26-3

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

CDU 340

Ficha catalográfica elaborada pela Biblioteca Reitor João Herculino

Centro Universitário de Brasília – UniCEUB
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

SUMÁRIO

PROBLEMAS GENÉRICOS DO DISCURSO JURÍDICO-PENAL NA [E SOBRE A] INTERNET E OUTROS CIBERESPAÇOS: UMA REVISÃO NARRATIVA DE LITERATURA SOBRE CRIMES

Rafael da Escóssia[1]

RESUMO

Este texto consiste numa revisão narrativa de parcela da literatura jurídico-penal na Internet sobre crimes digitais próprios e impróprios. Observou-se que os critérios classificatórios adotados pelos autores se fundam ora na qualidade analítica dos "meios virtuais" na construção do injusto penal (seja como elemento objetivo do tipo ou circunstância), ora na categoria do bem jurídico referenciado pela norma penal. Foram levantados problemas em relação ao entendimento desses meios e seu rendimento na habilitação de poder punitivo, assim como à pressuposição do caráter protetivo da norma penal e sua contribuição na elaboração do conceito de bem jurídico.

Palavras-chave: Crimes digitais. Teoria do delito. Teoria da pena. Bem jurídico.

ABSTRACT

This is a narrative review of part of the criminal law literature on 'propriate' and 'inappropriate' cybercrimes. It was observed that the classification criteria adopted by the authors are sometimes based on the cyberspace's analytical quality in the identification of the criminal infraction (either as type elements or circumstances),

[1] Bacharel em Direito na Universidade de Brasília (UnB); artista interdisciplinar; www.rafaeldaescossia.com; rafaeldaescossia@gmail.com. Aluno do curso de pós-graduação *lato sensu* em Direito Penal e Controle Social do Centro Universitário de Brasília – UniCEUB/ICDP.

or on the legal interest referred by the criminal law. Some problems were raised about the cyberspace's analytical understanding and its potential to enable punitive power, as well as about the law's protective goals and their contribution to the elaboration of the idea of 'legal interest'.

Keywords: Cybercrimes. Crime theory. Penalty theory. Legal interest.

1 INTRODUÇÃO

As novas dinâmicas de relacionamento na sociedade da informação possibilitam formas inovadoras de prática delitiva e de circulação e validação do discurso jurídico-penal. Na distinção entre crimes digitais próprios e impróprios, esta revisão narrativa de literatura levanta alguns problemas genéricos na formulação de parte desse discurso na contemporaneidade, com ênfase para sua relevância em termos de deslegitimação do poder punitivo do Estado.

2 METODOLOGIA

2.1 Questões preliminares

Parte-se do pressuposto político-pedagógico de que o discurso jurídico-penal se estrutura ao redor de saberes e práticas retóricas[2], mediante os quais se legitimam ficções de poder[3]. Essas ficções se contradizem com a eficácia intervertida no desempenho do poder punitivo na sociedade, que se orienta de maneira seletiva, estigmatizante[4] e necropolítica[5]. O saber dos juristas,

[2] PRANDO, Camila Cardoso de Mello. **O saber dos juristas e o controle penal**: o debate doutrinário na Revista de Direito (1933-1940) e a construção da legitimidade pela defesa social. Rio de Janeiro: Revan, 2013.

[3] MOMBAÇA, Jota. **Rumo a uma redistribuição desobediente de gênero e anticolonial da violência!** 2016, pp. 4-ss. Disponível em: https://issuu.com/amilcarpacker/docs/rumo_a_uma_redistribuic__a__o_da_vi. Acesso em: 27 de maio de 2020.

[4] Assim: ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; *et al*. **Direito Penal Brasileiro**: primeiro volume – Teoria Geral do Direito Penal. 4. ed. Rio de

mesmo em suas formulações mais críticas, não cumpre seu objetivo manifesto de contenção do desempenho das agências de criminalização[6] e se perde em contradições como o equilíbrio "entre a fundamentação da imputação e, logo, [a legitimação de] poder de punir, de um lado, e a delimitação da medida da pena, quando preenchidos os pressupostos para sua imposição"[7].

Em vista da situação crítica em que se encontra o sistema de justiça criminal[8] e as prioridades de um Estado que se diz "democrático e de direito", é de se questionar o rendimento **prático** de qualquer investigação dogmática. Com "prático" fala-se na capacidade real de exercício direto de poder deslegitimante ou nas possibilidades de elaboração de um discurso que seja disruptivo em relação aos cânones coloniais, ao buscar formas de se reimaginar o mundo que há de vir; sem, todavia, sucumbir às ficções de poder do mundo por acabar e ao desejo projetivo e controlador de oferecer alternativas[9].

Janeiro: Revan, 2013, p. 60. De toda forma, "a presença do racismo como fantasia colonial indeterminadamente atualizada no marco do colapso da colônia está exposta como ferida na paisagem das cidades, na densidade dos muros, cercas e fronteiras [...], na coreografia das carnes, na intensidade dos cortes e ancestralidade das cicatrizes". (MOMBAÇA, Jota. **Rumo a uma redistribuição desobediente de gênero e anticolonial da violência!** 2016, p. 4. Disponível em: https://issuu.com/amilcarpacker/docs/rumo_a_uma_redistribuic__a__o_da_vi. Acesso em: 27 de maio de 2020).

[5] Como em: MBEMBE, Achille. Necropolítica. In: **Arte & Ensaios**, Revista do PPGAV/EBA/UFRJ, n. 32, dez. 2016.

[6] ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; *et al*. **Direito Penal Brasileiro**: primeiro volume – Teoria Geral do Direito Penal. 4. ed. Rio de Janeiro: Revan, 2013, pp. 71-ss.

[7] TAVARES, Juarez. Culpabilidade e individualização da pena. In: BATISTA, Nilo; NASCIMENTO, André (orgs.). **Cem anos de reprovação**: uma contribuição transdisciplinar para a crise da culpabilidade. Rio de Janeiro: Revan, 2011, p. 137.

[8] Como se pode observar no "Levantamento Nacional de Informações Penitenciárias" de dezembro de 2019: https://app.powerbi.com/view?r=eyJrIjoiZTlkZGJjODQtNmJlMi00OTJhLWFlMDktNzRlNmFkNTM0MWI3IiwidCI6ImViMDkwNDIwLTQ0NGMtNDNmNy05MWYyLTRiOGRhNmJmZThlMSJ9. Acesso em: 18 de maio de 2020.

[9] MOMBAÇA, Jota. **Rumo a uma redistribuição desobediente de gênero e anticolonial da violência!** 2016, p. 16. Disponível em:

Considerando que a primeira opção não seja possível, resta a elaboração de um pensamento crítico que analise as próprias dinâmicas (meta)metodológicas de validação do discurso. Isso pode significar um esvaziamento teleológico da norma (como faz Zaffaroni em sua teoria negativa/agnóstica da pena[10]), algumas tentativas de reelaboração dessas práticas mediante processos híbridos/interdisciplinares[11] e literalmente **qualquer** preocupação com o método. Neste último caso, supõe-se uma disrupção quanto à tradição desse discurso e de suas agências de reprodução ideológica – embora, diga-se de passagem, não seja capaz de superar seu narcisismo, tampouco negar os presentes objetivos institucionais.[12]

2.2 Uma revisão narrativa de revisões narrativas

A revisão narrativa de literatura é um tipo amplo de publicação, indicado para descrever e discutir o desenvolvimento ou "estado da arte" de um determinado assunto, sob um ponto de vista teórico ou contextual. Trata-se, basicamente, da análise crítica de literatura publicada em artigos, ensaios, livros.[13] Embora

https://issuu.com/amilcarpacker/docs/rumo_a_uma_redistribuic__a__o_da_vi. Acesso em: 27 de maio de 2020.

[10] ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; *et al*. **Direito Penal Brasileiro**: primeiro volume – Teoria Geral do Direito Penal. 4. ed. Rio de Janeiro: Revan, 2013, p. 98.

[11] Por meio dos quais se podem negligenciar as infraestruturas coloniais de validação do conhecimento. Dessa forma: PRANDO, Camila Cardoso de Mello; BRAGA, Ana Gabriela. Práticas pedagógicas feministas e criminologia crítica: liberdade, transgressão e educação. **Boletim do IBCCrim**, ano 24, n. 280, março, 2016; KILOMBA, Grada. **Memórias da plantação**: Episódios de racismo cotidiano. 1. ed. Rio de Janeiro: Cobogó, 2019, p. 53; e PINACOTECA DE SÃO PAULO. **Roda de Conversa Grada Kilomba e Djamila Ribeiro**. 2019. Disponível em: https://www.youtube.com/watch?v=ovSKrDLs9Ro&t=999s. Acesso em: 10 fev. 2020.

[12] ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; *et al*. **Direito Penal Brasileiro**: primeiro volume – Teoria Geral do Direito Penal. 4. ed. Rio de Janeiro: Revan, 2013, pp. 69-73.

[13] ROTHER, Edna Terezinha. Revisão sistemática x revisão narrativa. **Acta Paulista de Enfermagem**, vol. 20, n. 2, São Paulo, abr./jun., 2007. Disponível em:

o método prescinda do rigor de uma revisão sistemática, optou-se aqui por explicitar as motivações, operações de pesquisa, critérios de seleção, lacunas e eventuais problemas identificáveis nas escolhas.

Mediante parâmetros obscuros para a grande maioria das pessoas (i.e., algoritmos), tecnologias como a Internet e as redes sociais alteram as formas de circulação do saber jurídico-penal e acesso a ele. Curiosamente, os mecanismos de busca *online* parecem transgredir os parâmetros tradicionais de validação acadêmica, privilegiando monografias de graduação, ensaios e "textos de opinião". Essa literatura vem ganhando relevo nos últimos tempos, seja porque pode ser acessada de maneira mais rápida e prática, seja porque sua publicação prescinde do esmero exigido por revistas com qualificações elevadas[14]. Isso pode significar que esses textos são até mais acessados – e, portanto, contribuem mais para a formação do imaginário jurídico geral – do que os tradicionais manuais de Direito. Como estes, os ensaios de Internet podem ser compreendidos como instrumentos de poder cultural que concorrem para a normalização do saber penal.[15]

Elegeu-se, assim, o Google como plataforma de busca.

Esta revisão de literatura se volta a um recorte desse discurso jurídico-penal, selecionado a partir das preferências ínsitas ao uso do dispositivo informático no qual realizei a pesquisa. Mediante diálogos com a produção teórica e crítica de Jota Mombaça, Achille Mbembe, Juarez Tavares, Eugenio Raúl

---

http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-21002007000200001. Acesso em: 29 de fevereiro de 2020.

[14] "Qualis", segundo os critérios da CAPES. A saber: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/veiculoPublicacaoQualis/listaConsultaGeralPeriodicos.jsfAcesso em: 27 de maio de 2020.

[15] BOURDIEU, Pierre. **O poder simbólico**. 15. ed. Rio de Janeiro: Bertrand Brasil, 2011.

Zaffaroni e Juarez Cirino dos Santos, foram levantados alguns problemas depreendidos da revisão. Não é objetivo deste texto oferecer "soluções" para esses problemas, mas questionar como a tradição do saber penal (consubstanciada nas teorias do delito e da pena) e os marcos teóricos se relacionam com o fragmento para mim editado dessa literatura na Internet.

3 REVISÃO NARRATIVA DE LITERATURA

No dia 5 de maio de 2020, foi realizada pesquisa no Google[16] mediante o termo de pesquisa "crimes digitais próprios e impróprios". Foram selecionados para revisão os 19 (dezenove) textos constantes das duas primeiras páginas de resultados. Para os fins desta pesquisa, os seguintes termos são tidos como sinônimos de "digitais": eletrônicos (*e-crimes*), informáticos, virtuais ou cibernéticos (cibercrimes, *cybercrimes*)[17]. O termo "crime" ou "delito", por sua vez, pode assumir diferentes sentidos. Considera-se aqui a conduta/ação típica, ilícita e culpável ou também o (tipo de) injusto culpável[18].

Os conceitos foram extraídos dos textos e suas eventuais referências bibliográficas, sistematizadas. Como "referências bibliográficas" foram considerados autores citados direta ou indiretamente nas definições. Na tabela a seguir, são indicados os textos por ordem de aparição no Google e suas referências. Foram

[16] Disponível em: https://www.google.com/search?q=crimes+digitais+pr%C3%B3prios+e+impr%C3%B3prios&rlz=1C5CHFA_enBR732BR732&oq=crimes+digitais+pr%C3%B3prios+e+impr%C3%B3prios&aqs=chrome.0.69i59l2j69i60l3j69i61.4611j0j4&sourceid=chrome&ie=UTF-8. Acesso em: 5 de maio de 2020.

[17] WIKIPÉDIA. **Crime informático**. Disponível em: https://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico. Acesso em: 5 de maio de 2020.

[18] TAVARES, Juarez. **Teoria do Delito**. São Paulo: Estúdio Editores.com, 2015, pp. 18-19; SANTOS, Juarez Cirino dos. **Direito Penal** – Parte Geral. 5. ed. Florianópolis: Conceito Editorial, 2012, p. 79.

destacados os textos que apenas apresentam citações de outros autores.

Tabela 1 – Textos revisados e suas eventuais referências na definição de crimes digitais próprios e impróprios

	TEXTOS	REFERÊNCIAS
1	CRESPO, Marcelo. **Crimes digitais: do que estamos falando?** Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/. 2015. Acesso em: 5 de maio de 2020.	Ele próprio.
2	FILGUEIRA, Matheus Henrique Balego; ORRIGO, Gabriel Marcos Achanjo**. Crimes cibernéticos**: uma abordagem jurídica sobre os crimes realizados no âmbito virtual. 2015. Disponível em: https://jus.com.br/artigos/43581/crimes-ciberneticos-uma-abordagem-juridica-sobre-os-crimes-realizados-no-ambito-virtual. Acesso em: 5 de maio de 2020.	Não há citação direta ou indireta na conceituação de crimes digitais próprios ou impróprios.
3	SCHIMIDT, Guilherme. **Crimes cibernéticos**. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. 2015. Acesso em: 5 de maio de 2020.	**Túlio Lima Vianna** *apud* Adeneele Garcia Carneiro
4	CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 5 de maio de 2020.	**Túlio Lima Vianna**; **Damásio de Jesus**
5	ALMEIDA, Maria Paula Castro. **A evolução no combate aos crimes digitais**. 2015. Disponível em: http://tiny.cc/fothoz. Acesso em: 5 de maio de 2020.	**Damásio de Jesus** *apud* Vladmir Aras
6	DURBANO, Vinicius. **Crimes cibernéticos:** saiba onde denunciar caso você seja vítima. 2019. Disponível em: https://ecoit.com.br/crimes-ciberneticos/. Acesso em: 5 de	Não há citação direta ou indireta na conceituação de

	maio de 2020.	crimes digitais próprios ou impróprios.
7	BORTOT, Jessica Fagundes. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. In: **VirtuaJus**, Belo Horizonte, v. 2, n. 2, pp. 338-362, 1º sem. 2017.	**Ivette Senise Ferreira**; **Vicente Greco Filho**
8	CAIADO, Felipe B; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**: coletânea de artigos, vol. 3. Brasília: MPF, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 5 de maio de 2020.	**Marcelo Crespo**
9	PANAZZOLO, Pedro de Vilhena. Racismo cibernético e os direitos da terceira dimensão. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**: coletânea de artigos, vol. 3. Brasília: MPF, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 5 de maio de 2020.	**Roberto Antônio Darós Malaquias**
10	OLIVEIRA, Beatris. **Direito Cibernético**. Você sabe o que é isso? 2019. Disponível em: https://www.catho.com.br/educacao/blog/direito-cibernetico-voce-sabe-o-que-e-isso/. Acesso em: 5 de maio de 2020.	Não há citação direta ou indireta na conceituação de crimes digitais próprios ou impróprios.
11	NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos**. 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em: 5 de maio de 2020.	**Damásio de Jesus** *apud* Adeneele Carneiro; **Túlio Vianna + Felipe**

		Machado
12	CARVALHO, Gabriel Chiovetto. **Crimes Cibernéticos**. 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/51878/crimes-ciberneticos. Acesso em: 5 de maio de 2020.	Não há citação direta ou indireta na conceituação de crimes digitais próprios ou impróprios.
13	MATSUYAMA, Keniche Guimarães. **Crimes cibernéticos**: atipicidade dos delitos. Disponível em: https://joaoademar.com.br/3cbpj.pdf. Acesso em: 5 de maio de 2020.	**Anderson Soares Furtado Oliveira**; **José Aires Rover**
14	FROTA, Jéssica Olivia Dias; PAIVA, Maria de Fátima Sampaio. Crimes Virtuais e as Dificuldades para Combatê-los. **In: ANAIS do IX Encontro de Pesquisa e Extensão da Faculdade Luciano Feijão**. Sobral-CE, novembro de 2017.	**Túlio Lima Vianna + Felipe Machado**
15	DORNELAS, Natália Alves. **A resposta estatal quanto aos crimes cibernéticos**: uma análise direcionada às Leis nº 12.735/2012 e 12.737/2012. 2019. 43p. Trabalho de Conclusão de Curso – Curso de Direito, UNIFACIG – Centro Universitário, Manhuaçu/MG, 2019.	**Túlio Lima Vianna + Felipe Machado**; **Augusto Rossini**; **Damásio de Jesus** *apud* Adeneele Carneiro
16	MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Vieira**. Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica**. 2012. Disponível em: http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2. Acesso em: 5 de maio de 2020.	Não há citação direta ou indireta na conceituação de crimes digitais próprios ou impróprios.
17	WIKIPÉDIA. **Crime informático**. Disponível em: https://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico.	**Túlio Lima Vianna**

	Acesso em: 5 de maio de 2020.	
18	MALHEIRO, Emerson Penha. **Delitos virtuais praticados na sociedade da informação**. 2017. Disponível em: http://www.rkladvocacia.com/delitos-virtuais-praticados-na-sociedade-da-informacao/. Acesso em: 5 de maio de 2020.	**Marcelo Crespo**; **Vicente Greco Filho**; **Emerson Vendt + Fábio Motta Lopes**
19	SANTOS, Izabella O'Hara Alves dos; CARVALHO, Grasielle Borges Vieira de. Atuação da Polícia Civil de Sergipe nos crimes contra a honra praticados em meio virtual. In: **Ciências Humanas e Sociais**, Aracaju, v. 4, n. 1, pp. 41-60, mar. 2017.	**Patrícia Santos da Silva**

Textos que apenas referenciam definições de outros autores.

Textos com conteúdo praticamente idêntico[19].

Os autores mais citados foram Túlio Lima Vianna (com ou sem Felipe Machado) (6 textos), Damásio de Jesus (4 textos), Marcelo Crespo (3 textos[20]) e Vicente Greco Filho (2 textos). Quando citados, os demais autores o são por apenas um texto.

Na sequência, procedeu-se à sistematização e agrupamento dos textos a partir dos critérios depreendidos na diferenciação de crimes digitais próprios impróprios pelos seus autores e/ou referências. Foram estabelecidas duas categorias: (i) autores que elaboram definições baseadas na essencialidade do meio virtual para prática do crime; e (ii) autores que distinguem os delitos pela necessidade do meio informático para a realização do crime e (ou somente) pela categoria dos bens jurídicos de referência das

[19] Enquanto o texto de Talles Nascimento apenas traz definições importadas de outros autores, o texto de Gabriel Carvalho lhe é praticamente idêntico.
[20] Marcelo Crespo cita a si mesmo.

normas. De forma geral, os autores foram confluentes no uso dos exemplos, mesmo adotando critérios classificatórios distintos.

3.1 A qualidade analítica do "meio virtual" na distinção entre crimes digitais próprios e impróprios

Roberto Darós Malaquias[21], José Aires Rover[22], Anderson Soares Oliveira[23], Beatris Oliveira, Patrícia Silva[24], Emmerson Wendt e Fábio Motta Lopes[25] compõem um primeiro grupo de autores cuja distinção entre crimes digitais próprios e impróprios é feita com base exclusiva na essencialidade da "tecnologia da informação e comunicação"/ "(sistema de) informática"/ "ambiente do ciberespaço"/Internet/ computador/"meio eletrônico" para a prática da conduta típica. Importante destacar que há uma diferença entre o "meio digital", Internet e computador/dispositivo informático.

Em vista do princípio da taxatividade dos enunciados ("pelo qual se exige que a definição da conduta criminosa indique, com

[21] PANAZZOLO, Pedro de Vilhena. Racismo cibernético e os direitos da terceira dimensão. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**: coletânea de artigos, vol. 3. Brasília: MPF, 2018, p. 119. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 5 de maio de 2020.

[22] MATSUYAMA, Keniche Guimarães. **Crimes cibernéticos**: atipicidade dos delitos. Disponível em: https://joaoademar.com.br/3cbpj.pdf, p. 4. Acesso em: 5 de maio de 2020.

[23] MATSUYAMA, Keniche Guimarães. **Crimes cibernéticos**: atipicidade dos delitos. Disponível em: https://joaoademar.com.br/3cbpj.pdf, p. 4. Acesso em: 5 de maio de 2020.

[24] SANTOS, Izabella O'Hara Alves dos; CARVALHO, Grasielle Borges Vieira de. Atuação da Polícia Civil de Sergipe nos crimes contra a honra praticados em meio virtual. In: **Ciências Humanas e Sociais**, Aracaju, v. 4, n. 1, pp. 41-60, mar. 2017, p. 46.

[25] MALHEIRO, Emerson Penha. **Delitos virtuais praticados na sociedade da informação**. 2017. Disponível em: http://www.rkladvocacia.com/delitos-virtuais-praticados-na-sociedade-da-informacao/. Acesso em: 5 de maio de 2020.

precisão, os elementos que a compõem"[26]), o uso do "computador" como meio ou instrumento para praticar uma ação não quer dizer, necessariamente, que se esteja diante de um crime digital, já que o dispositivo pode ser fisicamente movido para realizar inúmeros delitos, como o homicídio (art. 121, CP) e a lesão corporal (art. 129, CP). Vale o uso das preposições "com", "per" e "em"[27] para destacar essa diferença: crimes realizados *com* o computador ou *pelo/no* computador. "Crimes cibernéticos", portanto, seriam esses últimos caso "computador" seja entendido de maneira a abranger *smartphones*, *tablets* e outros dispositivos informáticos. O acesso à Internet não é essencial para essa caracterização, sendo que há operações possíveis no "meio eletrônico" sem que se faça uso da rede de computadores, como evidencia o próprio *caput* do art. 154-A do Código Penal (CP), incluído pela Lei n. 12.737/2012 (Lei dos Crimes Cibernéticos ou Lei Carolina Dieckmann[28]):

> Art. 154-A. Invadir dispositivo informático alheio, **conectado ou não à rede de computadores**, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. [...]

De toda forma, o cerne da distinção parece residir no *status* jurídico-dogmático da descrição do meio: seja como elemento objetivo do tipo ou circunstância. Por aquele se entende qualquer dado (descritivo ou normativo[29]) que não dependa, para sua

[26] TAVARES, Juarez. **Teoria do Delito**. São Paulo: Estúdio Editores.com, 2015, pp. 8 e 9.
[27] Ao se considerar os meios eletrônicos uma sorte de "espaço" ou "lugar" virtual.
[28] https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/. Acesso em: 12 de maio de 2020.
[29] Uma vez que toda interpretação comporta um juízo de valor, a distinção entre elementos descritivos e normativos do tipo objetivo soa pouco relevante.

existência (ou interpretação), da vontade do agente[30] e que, por óbvio, seja imprescindível para a caracterização da relação de tipicidade.

Como "circunstâncias (típicas)" podem ser reputadas as circunstâncias judiciais (art. 59, CP), legais (arts. 61, 62, 65 e 66, CP) e as causas de especial aumento ou diminuição de pena. Elas não fundamentam a existência jurídica do delito, mas podem interferir diretamente na habilitação do poder de punir. Exemplo é o § 4º do art. 122 do CP, em que a pena para o crime de induzimento, instigação ou auxílio a suicídio ou a automutilação é aumentada até o dobro se a conduta é realizada por meio da rede de computadores, de rede social ou transmitida em tempo real.

Outro exemplo importante da distinção entre elemento objetivo do tipo ou circunstância se encontra logo no primeiro artigo da Parte Especial do CP. Uma vez que se prove o "emprego de veneno, fogo, explosivo, asfixia, tortura ou outro meio insidioso ou cruel, ou de que possa resultar perigo comum" (art. 121, § 2°, III, CP), o homicídio se qualifica e, portanto, a ele se atribui uma nova cominação abstrata de pena. Verificando-se apenas essa qualificadora, sua identificação torna-se fundamental para a capitulação do crime – ou seja, é elemento objetivo do tipo de homicídio qualificado. Caso, todavia, haja mais de uma qualificadora e se opte pela desconsideração do inciso III do § 2° do art. 121, tais meios "insidiosos ou cruéis" passam a circundar a relação de tipicidade (assim como a própria caracterização do injusto), podendo ser valorados quando da aplicação da pena (art. 59 ou art. 61, II, d, CP).

[30] TAVARES, Juarez. **Teoria do Delito**. São Paulo: Estúdio Editores.com, 2015, p. 36.

Nesse ponto, Vicente Greco Filho lembra a distinção entre crimes de "conduta livre" e "conduta vinculada" para destacar essas diferenças. Segundo ele, nos delitos de conduta livre, "à lei importa apenas o evento modificador da natureza, como, por exemplo, o homicídio [simples]. O crime, no caso, é provocar o resultado morte, qualquer que tenha sido o meio ou a ação que o causou."[31]

Voltando ao art. 154-A do CP, o "meio eletrônico" é elemento do tipo objetivo, uma vez que a invasão de dispositivo informático, bem como a "violação de mecanismo de segurança" só podem acontecer virtualmente. Segundo o presente critério de classificação, a "criação e disseminação de vírus e outros códigos maliciosos, a invasão e a destruição de bancos de dados (público e privado)"[32] são crimes digitais próprios. Esse posicionamento é unânime entre os textos revisados.

Embora Emmerson Wendt e Fábio Motta Lopes[33] citem os delitos incluídos no Estatuto da Criança e do Adolescente (Lei n. 8.069/1990) pelas Leis n. 11.829/2008 e 12.015/2009 como crimes virtuais próprios, o uso do termo "sistema de informática ou telemático" no *caput* do art. 241-A é apenas exemplificativo de

[31] Em: BORTOT, Jessica Fagundes. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. In: **VirtuaJus**, Belo Horizonte, v. 2, n. 2, pp. 338-362, 1º sem. 2017, p. 342; e MALHEIRO, Emerson Penha. **Delitos virtuais praticados na sociedade da informação**. 2017. Disponível em: http://www.rkladvocacia.com/delitos-virtuais-praticados-na-sociedade-da-informacao/. Acesso em: 5 de maio de 2020.

[32] PANAZZOLO, Pedro de Vilhena. Racismo cibernético e os direitos da terceira dimensão. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**: coletânea de artigos, vol. 3. Brasília: MPF, 2018, p. 119. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 5 de maio de 2020.

[33] MALHEIRO, Emerson Penha. **Delitos virtuais praticados na sociedade da informação**. 2017. Disponível em: http://www.rkladvocacia.com/delitos-virtuais-praticados-na-sociedade-da-informacao/. Acesso em: 5 de maio de 2020.

quaisquer meios que possam ser utilizados para a prática das condutas.

> Art. 241-A. 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:
>
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
>
> § 1 º Nas mesmas penas incorre quem:
>
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o *caput* deste artigo;
>
> II – assegura, por qualquer meio, **o acesso por rede de computadores** às fotografias, cenas ou imagens de que trata o caput deste artigo.
>
> § 2 º As condutas tipificadas nos incisos I e II do § 1 º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.
>
> [...]
>
> Art. 244-B. Corromper ou facilitar a corrupção de menor de 18 (dezoito) anos, com ele praticando infração penal ou induzindo-o a praticá-la:
>
> Pena - reclusão, de 1 (um) a 4 (quatro) anos.
>
> § 1 º Incorre nas penas previstas no *caput* deste artigo quem pratica as condutas ali tipificadas utilizando-se de **quaisquer meios eletrônicos, inclusive salas de bate-papo da internet**.
>
> § 2 º As penas previstas no *caput* deste artigo são aumentadas de um terço no caso de a infração cometida ou induzida estar incluída no rol do art. 1 º da Lei n º 8.072, de 25 de julho de 1990.

Note-se a diferença em relação ao inciso II do § 1º do art. 241-A e ao § 1º do art. 244-B. Os parágrafos aditam os *caputs* para incluir, no primeiro caso, quem assegura o acesso **pela Internet** a cena de sexo explícito ou pornográfica envolvendo

menor de 18 anos e, no segundo, quem corrompe ou facilita a corrupção de menores por quaisquer meios **eletrônicos**. Em ambos os casos, essas condutas só podem se consubstanciar em meio digital. De acordo com a lógica da classificação em análise, considera-se que apenas nessas situações se está diante de crimes digitais próprios. Ou seja, os *caputs* dos art. 241-A e 244-B, assim como o inciso I do art. 241-A descrevem tipos digitais impróprios, da mesma forma que os crimes contra a honra (Título I, Cap. V, CP), os furtos (Título II, Cap. I, CP), o estelionato (art. 171, CP), a falsidade ideológica (art. 199, CP), a ameaça (art. 147, CP).

Não estando o meio virtual previsto como causa de especial aumento ou diminuição de pena (como no citado § 4º do art. 122 do CP), não há como afirmar de antemão até que ponto ele pode ser prejudicial ao réu. O mais importante, nesse caso, é se isso vai resultar mais ou menos pena nas duas primeiras fases da individualização (art. 68, CP), o que depende da valoração no caso concreto de tal circunstância perante as normas gerais contidas no CP.

Isso porque, como traz Ivette Senise Ferreira[34], "o sistema de informática ou o computador é um instrumento como tantos outros". Muito hoje acontece virtualmente (transações bancárias, compra e venda de produtos e serviços, reuniões, formação de carreira e agenciamentos, produção e divulgação de conteúdo, comunicação, etc.) e as condutas praticadas nesse espaço ou por

[34] BORTOT, Jessica Fagundes. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. In: **VirtuaJus**, Belo Horizonte, v. 2, n. 2, pp. 338-362, 1º sem. 2017, pp. 342-343.

meio dele influem diretamente nas nossas vidas, chegando, inclusive, a borrar seus contornos[35].

Caso, portanto, o meio eletrônico seja avaliado no cálculo da pena-base, ele pode contribuir para a construção do conteúdo de culpabilidade desde a gravidade subjetiva e objetiva da lesão ou perigo ao bem jurídico (conteúdo de injusto)[36]. Essa análise tem de levar em conta parâmetros relativamente objetivos de afetação do bem jurídico[37] que, por um lado, não representem dupla punição por elemento já considerado quando da fundamentação do juízo de imputação ou afirmação da responsabilidade; e, por outro, não reflitam meras idiossincrasias e preconceitos do órgão julgador. Dessa avaliação pode resultar mais ou menos pena.

[35] Isso não quer dizer que o discurso jurídico-penal compreenda facilmente a engenharia da conduta criminosa nesse meio, vez que o processo de imputação tradicionalmente recai sobre uma ação humana (independente do modelo de conduta adotado – causal, funcional, social, final, performático, etc.) (TAVARES, Juarez. **Teoria do Delito**. São Paulo: Estúdio Editores.com, 2015, pp. 20-ss) É um desafio de atualização para a dogmática e o processo penal contemporâneos estabelecer parâmetros mais ou menos seguros que permitam concluir que certa pessoa operou um dispositivo informático de determinada maneira a obter determinado resultado ilícito (ou se violou dever de cuidado ao realizar uma operação). Este texto, contudo, não vai se aprofundar no assunto.

[36] Uma vez que não seja possível desculpar a conduta por inimputabilidade, erro na consciência da ilicitude ou inexigibilidade de conduta diversa.

[37] Juarez Tavares elenca algumas referências extraídas da própria ordem jurídica, como a espécie de dolo (direto ou eventual) ou culpa (consciente ou inconsciente), "o processo de desenvolvimento da ação e seus limites, como tentativa, consumação ou exaurimento; o número de ações praticadas pelo agente e seus efeitos concretos; a facilidade ou dificuldade objetiva da execução; a ocorrência de fatores externos no processo de produção do resultado, como o efeito de condições naturais ou a atuação da vítima ou de terceiros, incluindo aquela das autoridades; a maior ou menor extensão do dano causado, em face do número de vítimas ou de bens lesados; o valor real dos bens lesados; a reparação do dano como forma limite de sua extensão; a duração do ato ilícito; a divisão de tarefas e o domínio da execução como autor, coautor, instigador ou partícipe; a relação objetiva do autor com a vítima, em termos de parentesco, indiferença, amizade ou inimizade; nos crimes omissivos, a qualidade do dever descumprido; nos crimes culposos, a forma e o modo de violação do dever de cuidado". Em: TAVARES, Juarez. Culpabilidade e individualização da pena. In: BATISTA, Nilo; NASCIMENTO, André (orgs.). **Cem anos de reprovação**: uma contribuição transdisciplinar para a crise da culpabilidade. Rio de Janeiro: Revan, 2011, pp. 142-147.

Ainda no art. 59, a prática da ação em meio virtual pode ser interpretada de forma latente para justificar a configuração de outras circunstâncias judiciais, que, diante dos ditames preventivos e protetivos da ordem jurídica, só podem ser invocadas em benefício do réu e "se situam fora do âmbito da avaliação acerca da gravidade do fato".[38]

Se a pena-base pode ter seu valor supostamente limitado pela culpabilidade, as circunstâncias legais agravantes e as causas de especial aumento atendem a outros ditames institucionais impostos pela lei em face da contundência política da relação do agente com o fato[39]. Embora obrigatória, a caracterização de qualquer uma delas no/pelo meio virtual está naturalmente subordinada à vedação do *bis in idem* e ao princípio do *in dubio pro reo*.

3.2 A espécie de bem jurídico referido pela norma penal como critério de distinção entre crimes digitais próprios e impróprios

De todos os autores, Marcelo Crespo[40] parece ser o único que defende uma distinção entre os crimes digitais próprios (ou de risco informático, como ele os chama) e impróprios com base

[38] Embora seja um posicionamento minoritário na doutrina e jurisprudência. Mais em: TAVARES, Juarez. Culpabilidade e individualização da pena. In: BATISTA, Nilo; NASCIMENTO, André (orgs.). **Cem anos de reprovação**: uma contribuição transdisciplinar para a crise da culpabilidade. Rio de Janeiro: Revan, 2011, pp. 133-ss.

[39] TAVARES, Juarez. Culpabilidade e individualização da pena. In: BATISTA, Nilo; NASCIMENTO, André (orgs.). **Cem anos de reprovação**: uma contribuição transdisciplinar para a crise da culpabilidade. Rio de Janeiro: Revan, 2011, pp. 139-140.

[40] Citado por: MALHEIRO, Emerson Penha. **Delitos virtuais praticados na sociedade da informação**. 2017. Disponível em: http://www.rkladvocacia.com/delitos-virtuais-praticados-na-sociedade-da-informacao/. Acesso em: 5 de maio de 2020; e CAIADO, Felipe B; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**: coletânea de artigos, vol. 3. Brasília: MPF, 2018, p. 16.

exclusiva na categoria do bem jurídico referenciado pela norma. Segundo ele, crimes digitais próprios (ou puros) são "condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra sistemas informáticos e os dados", enquanto os crimes digitais impróprios são "condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra bens jurídicos que não sejam tecnológicos, já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc.)".

Já Túlio Lima Vianna, Damásio de Jesus, Vicente Greco Filho, Maria Eugenia Mendes e Natália Vieira, Vinicius Durbano, Augusto Rossini, Matheus Balego Filgueira e Gabriel Archanjo Orrigo sustentam a posição majoritária depreendida dos textos revisados, em que a distinção em estudo se faz com base nos meios necessários para a realização do crime **e** na categoria do bem jurídico lesado ou posto em perigo.

Tabela 2 – Autores e suas definições do bem jurídico referido pelas normas penais que criminalizam os delitos virtuais próprios

AUTORES	DEFINIÇÕES
Túlio Lima Vianna (e Felipe Machado) [41]	*"inviolabilidade das informações automatizadas (dados)"*

[41] SCHIMIDT, Guilherme. **Crimes cibernéticos**. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. 2015. Acesso em: 5 de maio de 2020; CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 5 de maio de 2020; NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos**. 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em: 5 de maio de 2020; FROTA, Jéssica Olivia Dias; PAIVA, Maria de Fátima Sampaio. Crimes Virtuais e as Dificuldades para Combatê-los. In: **ANAIS do IX Encontro de Pesquisa e Extensão da Faculdade Luciano Feijão**. Sobral-CE, novembro de 2017, p. 5; DORNELAS, Natália Alves. **A resposta estatal quanto aos crimes cibernéticos**: uma análise direcionada às Leis nº 12.735/2012 e 12.737/2012. 2019. 43p. Trabalho de Conclusão de Curso – Curso de Direito, UNIFACIG – Centro Universitário, Manhuaçu/MG, 2019, pp. 10, 13 e 14; e WIKIPÉDIA. **Crime informático**. Disponível em:

Damásio de Jesus[42]	*"a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos)"*
Marcelo Crespo	*"sistemas informáticos e os dados"*
Vicente Greco Filho[43]	*"Internet"*
Maria Eugenia Mendes e Natália Vieira	*"informática"*
Vinicius Durbano	*"sistema informático"*
Augusto Rossini[44]	*"a segurança Informática, que tem por elementos a integridade, disponibilidade a confidencialidade"*
Matheus Balego Filgueira e Gabriel Archanjo Orrigo	*"os dados armazenados em outra máquina ou rede"*

Não obstante o esforço argumentativo dos autores na descrição desse suposto bem jurídico, sua caracterização se distancia da origem liberal do conceito (que hoje apresenta um

https://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico. Acesso em: 5 de maio de 2020.

[42] CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 5 de maio de 2020; ALMEIDA, Maria Paula Castro. **A evolução no combate aos crimes digitais**. 2015. Disponível em: http://tiny.cc/fothoz. Acesso em: 5 de maio de 2020; NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos**. 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em: 5 de maio de 2020; e DORNELAS, Natália Alves. **A resposta estatal quanto aos crimes cibernéticos**: uma análise direcionada às Leis nº 12.735/2012 e 12.737/2012. 2019. 43p. Trabalho de Conclusão de Curso – Curso de Direito, UNIFACIG – Centro Universitário, Manhuaçu/MG, 2019, p. 10 e pp. 13 e 14.

[43] MALHEIRO, Emerson Penha. **Delitos virtuais praticados na sociedade da informação**. 2017. Disponível em: http://www.rkladvocacia.com/delitos-virtuais-praticados-na-sociedade-da-informacao/. Acesso em: 5 de maio de 2020; BORTOT, Jessica Fagundes. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. In: **VirtuaJus**, Belo Horizonte, v. 2, n. 2, pp. 338-362, 1º sem. 2017, pp. 342-343.

[44] DORNELAS, Natália Alves. **A resposta estatal quanto aos crimes cibernéticos**: uma análise direcionada às Leis nº 12.735/2012 e 12.737/2012. 2019. 43p. Trabalho de Conclusão de Curso – Curso de Direito, UNIFACIG – Centro Universitário, Manhuaçu/MG, 2019, pp. 13 e 14.

suposto rendimento crítico em vista das novas formas de criminalização). Como descreve Juarez Tavares, a noção de bem-jurídico, ao longo do seu desenvolvimento na teoria do direito penal, "vai diluindo gradativamente sua substância material, até culminar praticamente na sua eliminação"[45].

Segundo a tese iluminista cunhada em 1801 por Feuerbach, o delito pressupunha a lesão a direito subjetivo, isto é, uma violação ao direito individual do ofendido de exercer sua liberdade em face da ação de outrem. Partia-se do pressuposto de um estado de igualdade de direitos entre os cidadãos (perspectiva contratual) e que a simples violação de um dever jurídico sancionado criminalmente não poderia ensejar a criminalização;[46] mas a pessoa portadora do direito subjetivo poderia exigir ou não a realização de uma conduta do indivíduo portador da obrigação[47].

Em 1834, o autor alemão Birnbaum, sob a necessidade de adequar a teoria do delito às normas penais vigentes em seu país (que criminalizavam crimes contra o Estado, a religião e a comunidade), cunhou a ideia de bem jurídico, que começou a se distanciar dos pressupostos originários de sua validade na habilitação da pena. Esse movimento, como propõe Nilo Batista, pode ser comparado às próprias evoluções do capitalismo. Num primeiro momento, como bem material, o conceito surge no contexto da grande produção e do incremento de consumo na Europa (capitalismo industrial) e vai gradualmente perdendo sua substância material, até ser enunciado por Binding como mero pressuposto formal da norma incriminadora (capitalismo

[45] TAVARES, Juarez. **Teoria do Injusto Penal**. 3. ed. Belo Horizonte: Del Rey, 2003, p. 197.
[46] TAVARES, Juarez. **Teoria do Injusto Penal**. 3. ed. Belo Horizonte: Del Rey, 2003, p. 183.
[47] TAVARES, Juarez. **Teoria do Delito**. São Paulo: Estúdio Editores.com, 2015, p. 10.

financeiro) ou ainda como função (capitalismo de serviços) ou estabilidade normativa (segundo a visão pós-moderna do funcionalismo).[48] Com a criminalidade virtual, "bem jurídico" ganha um nova dimensão dogmática, confundindo-se, segundo argumentam os textos revisados, com a própria Internet ou os "dados eletrônicos".

Tal espiritualização do bem jurídico pode, inclusive, levar à confusão na noção de "resultado", como se observa na escrita de Damásio de Jesus[49]:

> [...] os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço 'real', ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

A doutrina costuma distinguir os crimes quanto aos efeitos da conduta. Disso deriva uma outra classificação, agora entre os chamados "crimes materiais" (ou de resultado), "formais" ou de "mera conduta". Essa diferença "corresponde à relação entre a ação e a modificação do mundo exterior, de tal sorte que se possa proceder a uma delimitação naturalística" entre as categoriais. Enquanto nos crimes materiais seria possível distinguir entre a ação e seus efeitos sensíveis "no mundo" (resultado naturalístico); nos outros a lei prescindiria da indicação de tais efeitos.[50] Segundo

[48] TAVARES, Juarez. **Teoria do Injusto Penal**. 3. ed. Belo Horizonte: Del Rey, 2003, pp. 185-186.

[49] Em: ALMEIDA, Maria Paula Castro. **A evolução no combate aos crimes digitais**. 2015. Disponível em: http://tiny.cc/fothoz. Acesso em: 5 de maio de 2020; CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. 2012. Acesso em: 5 de maio de 2020; e NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos**. 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em: 5 de maio de 2020.

[50] TAVARES, Juarez. **Teoria do Delito**. São Paulo: Estúdio Editores.com, 2015, p. 38.

Claus Roxin, o resultado estaria separado espacial e temporalmente da conduta nos delitos materiais.[51]

Ocorre que, segundo o princípio da lesividade, o pressuposto de aplicação e execução das penas é o perigo ou a lesão significativa a bem jurídico[52], isto é, o resultado necessário para a configuração do conteúdo de injusto da conduta (núcleo conceitual do crime)[53]. Mesmo em delitos sem resultado naturalístico exigido pela norma, como nos crimes contra a honra (virtuais impróprios), é possível atestar (e contestar) os efeitos deletérios à pessoa de que podem resultar os atos injuriosos, caluniosos ou difamatórios nas redes sociais, por exemplo. Trata-se do reconhecimento desse bem jurídico e de que certas condutas podem de fato lesioná-lo e promover alterações no mundo, mesmo que a conduta criminosa não produza efeitos sensíveis sobre determinado objeto.

Nesse ponto, Juarez Tavares observa a diferença entre "bem jurídico" e "objeto da ação" ou objeto material.[54] A figura do crime impossível (art. 17, CP), inclusive, parte do tácito reconhecimento de que existem objetos materiais desprovidos de bem jurídico ("impropriedade absoluta do objeto"). O corpo, por exemplo, não se confunde com a vida; nem a coisa, com a propriedade. Aqui a formulação originária de Ludwig Feuerbach poderia oferecer uma contribuição para distinguir bens jurídicos "legítimos" de construções retóricas. Não se trata propriamente da existência ou não de objeto material, mas de uma referência mínima à violação da liberdade pactuada (em tese) isonômica e socialmente, cuja

[51] ROXIN, Claus. **Derecho Penal**: Parte General, Tomo I. Madrid: Civitas, 1997, § 10, 102, p. 328.

[52] SANTOS, Juarez Cirino dos. **Direito Penal** – Parte Geral. 5. ed. Florianópolis: Conceito Editorial, 2012, p. 26.

[53] TAVARES, Juarez. **Teoria do Delito**. São Paulo: Estúdio Editores.com, 2015, pp. 37-38.

[54] TAVARES, Juarez. **Teoria do Injusto Penal**. 3. ed. Belo Horizonte: Del Rey, 2003, pp. 226-ss.

lesão ou ameaça a direito não se excluirá da apreciação do Poder Judiciário (art. 5º, XXXV, CF). Em outras palavras, o que importa não é a existência de resultado naturalístico, mas a sua relação com a afetação do bem jurídico, entendido como pressuposto de incriminação.[55] Nesse sentido, todo delito tem resultado.[56]

A imprecisão de Damásio ao conceituar o bem jurídico "informático" mediante a ausência de resultado naturalístico parece sugerir uma dificuldade teórica e dogmática na compreensão desses novos delitos, assim como dos próprios fundamentos estruturais da teoria do crime a partir do Brasil e da América Latina. As origens europeias do discurso atritam com os regimes assimétricos de distribuição de violência e privilégio na sociedade colonial, resultando em certas premissas ficcionais, tais como **(i)** a programação legal da criminalização secundária e **(ii)** a idoneidade da norma penal na proteção de bens, valores ou direitos (e, por extensão, a eventual faculdade limitadora da dogmática).

i. Observa-se que a construção da norma penal (e, por sua vez, do discurso jurídico sobre ela) tem como referência o Estado europeu, cuja ordem jurídica de inscrição (*jus publicum europaeum*) fundou-se a partir de dois princípios-chave: a igualdade jurídica aos Estados (como modelos "de unidade política, princípios de organização racional, personificação da ideia universal e símbolos de moralidade"); e a territorialização do Estado soberano. [57] Embora anterior à formulação de Feuerbach sobre direitos subjetivos, essa concepção de soberania em muito se lhe

[55] TAVARES, Juarez. **Teoria do Delito**. São Paulo: Estúdio Editores.com, 2015, p. 40.
[56] ROXIN, Claus. **Derecho Penal**: Parte General, Tomo I. Madrid: Civitas, 1997, § 10, 104, p. 329.
[57] MBEMBE, Achille. Necropolítica. In: **Arte & Ensaios**, Revista do PPGAV/EBA/UFRJ, n. 32, dez. 2016, pp. 133 e 135.

assemelha sobretudo em face dos pressupostos compartilhados de igualdade, que, em síntese, implicam um **reconhecimento** mútuo entre Estados ou pessoas.

Como desdobramento dos princípios-chave do *jus publicum europaeum*, advém a importante faculdade de o Estado negociar a guerra e a paz (o direito de guerra). Isso implicava que ele não poderia fazer reinvindicações para além de suas fronteiras, mas não reconheceria, em seu território, nenhuma autoridade maior. O Estado, ainda, se "comprometeria a 'civilizar' os modos de matar e atribuir objetivos racionais ao ato de matar em si".[58] De forma semelhante, a pessoa pode dispor sobre seu próprio corpo, mas, de forma geral, não é lícito a outrem violá-lo.

Como descreve Achille Mbembe[59], uma consequência importante da territorialização da soberania do Estado foi a formação de duas ordens paralelas: a europeia (sob a imperatividade do *jus publicum*) e o resto do mundo, sujeito à apropriação colonial. De um lado, portanto, há a guerra legítima entre Estados "civilizados"; de outro, um perene estado de exceção na colônia, que é zona de "hostilidade absoluta que coloca o conquistador contra o inimigo absoluto". Diante de uma vasta maioria de mortos-vivos, o *status* político de ser humano é privilégio de alguns poucos na sociedade colonial.

Considerando que o fantasma da escravidão, o racismo e a supremacia branca permanecem como eixos estruturantes do funcionamento necropolítico do sistema de justiça criminal

[58] MBEMBE, Achille. Necropolítica. In: **Arte & Ensaios**, Revista do PPGAV/EBA/UFRJ, n. 32, dez. 2016, p. 133.
[59] MBEMBE, Achille. Necropolítica. In: **Arte & Ensaios**, Revista do PPGAV/EBA/UFRJ, n. 32, dez. 2016, pp. 124 e 133-134.

brasileiro[60], não é possível distinguir com clareza o "inimigo" do "criminoso" na colônia, onde o "direito" soberano de matar não está submetido a qualquer regra, não há distinção entre guerra e paz, o massacre e a burocracia sintetizam-se.[61]

Enquanto o desenvolvimento da doutrina penal permanece assentado em suas origens liberais e europeias – o que promove toda a orientação epistemológica e política da doutrina, a dedução da teoria do direito penal e a assunção de um suposto "direito penal subjetivo" (*jus puniendi*) de tutularidade do Estado[62] –, o poder bélico está orientado pelo "desejo de gerir e performar a violência não apenas ao estado"[63] e à lei.

O discurso jurídico-penal habita um mundo imaginário em que a máxima expressão da soberania é a produção de normas gerais por sujeitos livre e iguais, capazes de autoconhecimento, autoconsciência e autorrepresentação.[64] Como descreve Zaffaroni[65], um dos paradoxos desse saber consiste em oferecer supostos parâmetros de racionalização para a aplicação da lei, mas, ao cabo, legitimar um poder à margem dela.

---

[60] MOMBAÇA, Jota. **Rumo a uma redistribuição desobediente de gênero e anticolonial da violência!** Disponível em: https://issuu.com/amilcarpacker/docs/rumo_a_uma_redistribuic__a__o_da_vi. 2016, p. 6. Acesso em: 27 de maio de 2020, p. 3.

[61] MBEMBE, Achille. Necropolítica. In: **Arte & Ensaios**, Revista do PPGAV/EBA/UFRJ, n. 32, dez. 2016, p. 132.

[62] ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro. **Direito Penal Brasileiro**: primeiro volume – Teoria Geral do Direito Penal. 4. ed. Rio de Janeiro: Revan, 2013, pp. 97-98.

[63] MOMBAÇA, Jota. **Rumo a uma redistribuição desobediente de gênero e anticolonial da violência!** Disponível em: https://issuu.com/amilcarpacker/docs/rumo_a_uma_redistribuic__a__o_da_vi. 2016, p. 6. Acesso em: 27 de maio de 2020.

[64] MBEMBE, Achille. Necropolítica. In: **Arte & Ensaios**, Revista do PPGAV/EBA/UFRJ, n. 32, dez. 2016, p. 124.

[65] ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro. **Direito Penal Brasileiro**: primeiro volume – Teoria Geral do Direito Penal. 4. ed. Rio de Janeiro: Revan, 2013, p. 71.

ii. O pressuposto protetivo da norma penal é a segunda premissa ficcional a partir de que se enumeram problemas na compreensão da teoria do bem jurídico desde o Brasil. Em todos os textos revisados foram utilizados os termos "tutela" ou "proteção" para definir a relação da norma penal com seu objeto jurídico. Essa assunção é problemática.

Uma vez que se identificam critérios racistas e classistas na seleção realizada pelo sistema de justiça criminal, pode-se sugerir que a habilitação de violência ocorre de maneira a garantir a segurança e o privilégio de um certo outro grupo de pessoas[66], enquanto (no mínimo) zonas de imunidade (ou invulnerabilidade) perante as agências punitivas.[67] Da mesma forma que o racismo se constrói a partir da branquitude como ponto de referência a partir de que todas/os as/os 'Outras/os' diferem[68], a violência penal é arbitrada segundo a ficção de que a "racionalidade da vida passa pela morte do outro; ou que a soberania consiste na vontade e capacidade de matar para possibilitar viver"[69].

Em consequência, isso poderia ser enunciado da seguinte forma: a norma penal protege bens jurídicos, mas não são todos, nem de qualquer um. Ela protege os bens jurídicos dos herdeiros dos privilégios coloniais, isto é, as pessoas brancas e ricas, sobretudo. Nesse ponto, Juarez Cirino dos Santos, mediante uma interpretação do direito penal influenciada pela tradição marxista,

---

[66] MOMBAÇA, Jota. **Rumo a uma redistribuição desobediente de gênero e anticolonial da violência!** Disponível em: https://issuu.com/amilcarpacker/docs/rumo_a_uma_redistribuic__a__o_da_vi. 2016, p. 6. Acesso em: 27 de maio de 2020, p. 3.

[67] ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro. **Direito Penal Brasileiro**: primeiro volume – Teoria Geral do Direito Penal. 4. ed. Rio de Janeiro: Revan, 2013, pp. 46-ss.

[68] KILOMBA, Grada. **Memórias da plantação**: Episódios de racismo cotidiano. 1. ed. Rio de Janeiro: Cobogó, 2019, p. 75.

[69] MBEMBE, Achille. Necropolítica. In: **Arte & Ensaios**, Revista do PPGAV/EBA/UFRJ, n. 32, dez. 2016, pp. 128-129.

reconhece objetivos latentes (ou reais) à norma penal, entre eles a "proteção das condições fundamentais da sociedade de produção de mercadorias", isto é, a proteção das relações sociais desiguais, mediante garantia da relação capital/trabalho assalariado. Essa proteção é seletiva dos bens jurídicos das classes e grupos sociais hegemônicos, o que pré-seleciona os sujeitos estigmatizáveis pela sanção penal (ou seja, os contingentes marginalizados do mercado de trabalho e do consumo social).[70]

Uma outra crítica à eventual proteção conferida pela norma penal seria o caráter pós-fático da sua intervenção, característica própria do modelo punitivo de decisão de conflito – que não o resolve; mas o suspende no tempo e cria um novo, que se confunde com a própria criminalização.[71] O bem jurídico, assim, seria um objeto ou critério de preferência e referência da norma, uma vez que a habilitação de poder de punir só seria válida (e eficaz) na medida em que fosse provada uma lesão ou perigo a um bem jurídico.[72]

Já que não se trata de uma proteção efetiva, portanto, qual seria o tipo de tutela que a norma conferiria aos bens jurídicos? Supondo que seja uma tutela simbólica, a análise de sua validade pode ser feita em conjunto com o art. 59 do CP, que determina que a fixação de pena deverá ser realizada "conforme seja necessário e suficiente para reprovação e prevenção do crime".

Tradicionalmente o discurso jurídico-penal vem atribuindo diversas funções preventivas para a pena, tais como a

[70] SANTOS, Juarez Cirino dos. Direito Penal – Parte Geral. 5. ed. Florianópolis: Conceito Editorial, 2012, pp. 11 e 17.
[71] ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro. **Direito Penal Brasileiro**: primeiro volume – Teoria Geral do Direito Penal. 4. ed. Rio de Janeiro: Revan, 2013, p. 87.
[72] TAVARES, Juarez. **Teoria do Injusto Penal**. 3. ed. Belo Horizonte: Del Rey, 2003, p. 205.

ressocialização (prevenção especial positiva), a intimidação/dissuasão (prevenção geral negativa), a neutralização/eliminação do criminoso (prevenção especial negativa) e o reforço simbólico da confiança na norma (prevenção geral positiva)[73].

A Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), todavia, que atualmente é vinculante para os Estados membros da Organização dos Estados Americanos (OEA), da qual o Brasil faz parte, indica, em seu artigo 5.6, que a reforma e a readaptação dos condenados, como finalidade essencial das penas privativas de liberdade, são garantias da segurança cidadã e direitos das pessoas privadas de liberdade. Como norma supralegal, ela prevalece sobre o art. 59 do CP, balizando o entendimento de "prevenção"[74] enquanto reparação da inferioridade perigosa, melhoramento moral da pessoa[75] ou ainda, segundo a Lei de Execução Penal, "harmônica integração social do condenado ou internado" (art. 1º).

Ocorre que o Conselho Nacional de Justiça, em 2019, informou "*que no mínimo, 42,5% das pessoas com processos registrados nos Tribunais de Justiça em 2015 de todo o Brasil reentraram no Poder Judiciário até dezembro de 2019*"[76]. O dado é sintoma de que – como concluiu a Comissão Interamericana de

[73] ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro. **Direito Penal Brasileiro**: primeiro volume – Teoria Geral do Direito Penal. 4. ed. Rio de Janeiro: Revan, 2013, pp. 115-116.

[74] LIMA, Rafael da Escóssia; MOREIRA, Leonardo de Melo. **Encarceramento no Brasil não cumpre função ressocializadora**. Disponível em: https://www.conjur.com.br/2016-jan01/encarceramento-brasil-nao-cumpre-funcao-ressocializadora. Acesso em: 3 de junho de 2020.

[75] ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro. **Direito Penal Brasileiro**: primeiro volume – Teoria Geral do Direito Penal. 4. ed. Rio de Janeiro: Revan, 2013, p. 116.

[76] BRASIL. CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Reentradas e reinterações infracionais**: um olhar sobre os sistemas socioeducativo e prisional brasileiros. Brasília: CNJ, 2019, p. 52.

Direitos Humanos em 2011 – as sérias deficiências estruturais no sistema prisional brasileiro afetam direitos humanos como a vida e a integridade pessoal dos reclusos, assim como impedem que as penas privativas de liberdade cumpram com a finalidade essencial prescrita pela Convenção Interamericana sobre Direitos Humanos[77].

Ainda que seja reconhecida uma proteção simbólica dos bens jurídicos (na forma de prevenção geral do delito), ela não está autorizada pela ordem jurídica como fundamento para a habilitação de pena. Se, por outro lado, compreendido o termo "prevenção" enquanto "ressocialização", os dados de funcionamento do sistema de justiça criminal não apenas o refutam, mas indicam a eficácia invertida do cárcere, que dessocializa, estigmatiza e reforça zonas de vulnerabilidade perante a situação de perigo penal.[78]

Ao menos sob o ponto de vista teórico, as perspectivas críticas apresentadas indicam que as garantias constitucionais à não-discriminação (art. 2º, IV) e proteção à pessoa (art. 1º, III) vão de encontro à função protetiva da norma penal – o que, por si só, tem o condão de reestruturar de maneira muito importante a teoria do delito e a própria compreensão de seus institutos.

Por fim, vale destacar que, como os demais elementos do tipo (e a não configuração de alguma excludente de ilicitude ou culpabilidade), o conceito de bem jurídico tem de ser dotado de mínima substancialidade, de forma que sua lesão ou perigo

[77] COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Informe sobre los derechos humanos de las personas privadas de libertad en las Américas**. OEA/Ser.L/V/II. Doc. 64. 31 deciembre 2011, prefacio. Disponível em: www.cidh.org. Acesso em: 18 de maio de 2020.

[78] LIMA, Rafael da Escóssia; MOREIRA, Leonardo de Melo. **Encarceramento no Brasil não cumpre função ressocializadora**. Disponível em: https://www.conjur.com.br/2016-jan01/encarceramento-brasil-nao-cumpre-funcao-ressocializadora. Acesso em: 3 de junho de 2020.

estejam sujeitos a um procedimento de demonstração e, de maneira ainda mais importante, de contestação ou refutação[79] em respeito aos princípios do contraditório e ampla defesa (art. 5º, LV, CF).

4 CONCLUSÃO

Realizou-se revisão narrativa de recorte da literatura jurídico-penal na Internet sobre os chamados "crimes digitais próprios e impróprios", de forma a compreender os critérios adotados pelos autores em sua distinção. Para fins de contenção do poder punitivo do Estado, propôs-se um pensamento crítico quanto aos textos revisados, dialogando com formulações latino-americanas dissidentes em relação ao discurso jurídico-penal hegemônico.

Em parte dos textos, verificou-se que a distinção foi proposta a partir da qualidade analítico-dogmática do "meio virtual", seja como elemento do tipo objetivo (crimes digitais próprios) ou circunstância (crimes digitais impróprios). Neste caso, é importante considerar que a avaliação dos meios eletrônicos na (des)habilitação de pena deve ser analisada caso a caso – seja em face das causas de especial aumento ou diminuição, seja diante das normas gerais previstas no CP (circunstâncias judiciais ou legais).

Outra parte dos autores distinguiu os delitos virtuais com base na espécie de bem jurídico referenciado pela norma. Os crimes digitais próprios seriam aqueles cujo bem jurídico de referência são os "dados armazenados eletronicamente", o que, conforme analisado, ressalta os problemas históricos de gradual espiritualização do conceito de bem jurídico e perda de seu

[79] TAVARES, Juarez. **Teoria do Injusto Penal**. 3. ed. Belo Horizonte: Del Rey, 2003, pp. 220-221.

rendimento na proteção ao acusado/investigado. Vale destacar que todas as etapas do processo de imputação devem estar sujeitas à possibilidade de refutação, em atendimento aos princípios do contraditório e da ampla defesa.

Diante dos problemas identificados na compreensão dos institutos tradicionais de Direito Penal pela parcela revisada do discurso jurídico na (e sobre a) Internet (e outros ciberespaços), restam dúvidas sobre a relevância pedagógica das "taxonomias dos crimes" – tão numerosas quanto queira quem as cria.

REFERÊNCIAS

ALMEIDA, Maria Paula Castro. **A evolução no combate aos crimes digitais**. 2015. Disponível em: http://tiny.cc/fothoz. Acesso em: 5 de maio de 2020.

BOURDIEU, Pierre. **O poder simbólico***.* 15. ed. Rio de Janeiro: Bertrand Brasil, 2011.

BORTOT, Jessica Fagundes. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. In: **VirtuaJus**, Belo Horizonte, v. 2, n. 2, pp. 338-362, 1º sem. 2017.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Reentradas e reinterações infracionais**: um olhar sobre os sistemas socioeducativo e prisional brasileiros. Brasília: CNJ, 2019.

CAIADO, Felipe B; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**: coletânea de artigos, vol. 3. Brasília: MPF, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 5 de maio de 2020.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. 2012.

Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 5 de maio de 2020.

CARVALHO, Gabriel Chiovetto. **Crimes Cibernéticos**. 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/51878/crimes-ciberneticos. Acesso em: 5 de maio de 2020.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Informe sobre los derechos humanos de las personas privadas de libertad en las Américas**. OEA/Ser.L/V/II. Doc. 64. 31 deciembre 2011, prefacio. Disponível em: www.cidh.org. Acesso em: 18 de maio de 2020.

CRESPO, Marcelo. **Crimes digitais: do que estamos falando?** Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/. 2015. Acesso em: 5 de maio de 2020.

DORNELAS, Natália Alves. **A resposta estatal quanto aos crimes cibernéticos**: uma análise direcionada às Leis nº 12.735/2012 e 12.737/2012. 2019. 43p. Trabalho de Conclusão de Curso – Curso de Direito, UNIFACIG – Centro Universitário, Manhuaçu/MG, 2019.

DURBANO, Vinicius. **Crimes cibernéticos:** saiba onde denunciar caso você seja vítima. 2019. Disponível em: https://ecoit.com.br/crimes-ciberneticos/. Acesso em: 5 de maio de 2020.

FILGUEIRA, Matheus Henrique Balego; ORRIGO, Gabriel Marcos Achanjo**. Crimes cibernéticos**: uma abordagem jurídica sobre os crimes realizados no âmbito virtual. 2015. Disponível em: https://jus.com.br/artigos/43581/crimes-ciberneticos-uma-abordagem-juridica-sobre-os-crimes-realizados-no-ambito-virtual. Acesso em: 5 de maio de 2020.

FROTA, Jéssica Olivia Dias; PAIVA, Maria de Fátima Sampaio. Crimes Virtuais e as Dificuldades para Combatê-los. **In: ANAIS do IX Encontro de Pesquisa e Extensão da Faculdade Luciano Feijão**. Sobral-CE, novembro de 2017.

KILOMBA, Grada. **Memórias da plantação**: Episódios de racismo cotidiano. 1. ed. Rio de Janeiro: Cobogó, 2019.

LIMA, Rafael da Escóssia; MOREIRA, Leonardo de Melo. **Encarceramento no Brasil não cumpre função ressocializadora**. Disponível em: https://www.conjur.com.br/2016-jan01/encarceramento-brasil-nao-cumpre-funcao-ressocializadora. Acesso em: 3 de junho de 2020.

MALHEIRO, Emerson Penha. **Delitos virtuais praticados na sociedade da informação**. 2017. Disponível em: http://www.rkladvocacia.com/delitos-virtuais-praticados-na-sociedade-da-informacao/. Acesso em: 5 de maio de 2020.

MATSUYAMA, Keniche Guimarães. **Crimes cibernéticos**: atipicidade dos delitos. Disponível em: https://joaoademar.com.br/3cbpj.pdf. Acesso em: 5 de maio de 2020.

MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Vieira**. Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica**. 2012. Disponível em: http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2. Acesso em: 5 de maio de 2020.

MOMBAÇA, Jota. **Rumo a uma redistribuição desobediente de gênero e anticolonial da violência!** Disponível em: https://issuu.com/amilcarpacker/docs/rumo_a_uma_redistribuic__a__o_da_vi. 2016. Acesso em: 27 de maio de 2020.

NASCIMENTO, Talles Leandro Ramos. **Crimes cibernéticos**. 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em: 5 de maio de 2020.

OLIVEIRA, Beatris. **Direito Cibernético**. Você sabe o que é isso? 2019. Disponível em: https://www.catho.com.br/educacao/blog/direito-cibernetico-voce-sabe-o-que-e-isso/. Acesso em: 5 de maio de 2020.

PANAZZOLO, Pedro de Vilhena. Racismo cibernético e os direitos da terceira dimensão. In: BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão. **Crimes cibernéticos**: coletânea de artigos, vol. 3. Brasília: MPF, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-

artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 5 de maio de 2020.

PINACOTECA DE SÃO PAULO. **Roda de Conversa Grada Kilomba e Djamila Ribeiro**. 2019. Disponível em: https://www.youtube.com/watch?v=ovSKrDLs9Ro&t=999s. Acesso em: 10 fev. 2020.

PRANDO, Camila Cardoso de Mello. **O saber dos juristas e o controle penal**: o debate doutrinário na Revista de Direito (1933-1940) e a construção da legitimidade pela defesa social. Rio de Janeiro: Revan, 2013.

_____; BRAGA, Ana Gabriela. Práticas pedagógicas feministas e criminologia crítica: liberdade, transgressão e educação. **Boletim do IBCCrim**, ano 24, n. 280, março, 2016.

ROTHER, Edna Terezinha. Revisão sistemática x revisão narrativa. **Acta Paulista de Enfermagem**, vol. 20, n. 2, São Paulo, abr./jun., 2007. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-21002007000200001. Acesso em: 29 de fevereiro de 2020.

ROXIN, Claus. **Derecho Penal**: Parte General, Tomo I. Madrid: Civitas, 1997.

SANTOS, Izabella O'Hara Alves dos; CARVALHO, Grasielle Borges Vieira de. Atuação da Polícia Civil de Sergipe nos crimes contra a honra praticados em meio virtual. In: **Ciências Humanas e Sociais**, Aracaju, v. 4, n. 1, p. 41-60, mar. 2017.

SANTOS, Juarez Cirino dos. **Direito Penal** – Parte Geral. 5. ed. Florianópolis: Conceito Editorial, 2012.

SCHIMIDT, Guilherme. **Crimes cibernéticos**. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. 2015. Acesso em: 5 de maio de 2020.

TAVARES, Juarez. **Teoria do Delito**. São Paulo: Estúdio Editores.com, 2015.

_____. Culpabilidade e individualização da pena. In: BATISTA, Nilo; NASCIMENTO, André (orgs.). **Cem anos de reprovação**: uma contribuição transdisciplinar para a crise da culpabilidade. Rio de Janeiro: Revan, 2011.

_____. **Teoria do Injusto Penal**. 3. ed. Belo Horizonte: Del Rey, 2003.

WIKIPÉDIA. **Crime informático**. Disponível em: https://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico. Acesso em: 5 de maio de 2020.

ZAFFARONI, Eugenio Raú; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro. **Direito Penal Brasileiro**: primeiro volume – Teoria Geral do Direito Penal. 4. ed. Rio de Janeiro: Revan, 2013.

CRIMES PRÓPRIOS E IMPRÓPRIOS DO MEIO DIGITAL

José Pires Mesquita Filho[1]

RESUMO

O objetivo do presente artigo é esclarecer as formas de cometimento dos crimes cibernéticos que, após a facilidade de acesso a informação, independente da classe social, vem aumentando absurdamente com o avanço tecnológico cada vez mais aguçado, abrindo caminhos para a prática de novos crimes. A sociedade hoje é a "Sociedade da Informação" e da pós guerra, onde a revolução tecnológica trouxe muitos benefícios e comodidade para as pessoas, mas, também acarretou a transformação das relações sociais, haja vista o uso do meio virtual para cometimento do crime, seja ele próprio ou impróprio.

Palavras-chave: Crimes. Informação. Digital.

ABSTRACT

The aim of this article is to clarify the ways of committing cybercrimes that, after the ease of access to information, regardless of social class, has been increasing absurdly, with technological advances increasingly pointed, paving the way for the practice of new crimes. Society today is the "Information Society" and the post-war, where the technological revolution brought many benefits and convenience to people, but also led to the transformation of social relations, given the use of the virtual medium for committing crime, whether itself or improper.

Keywords: Crimes. Information. Digital.

---

[1] Aluno da Pós-Graduação *lato sensu* em Direito do Instituto Ceub de Pesquisa e Desenvolvimento do Centro Universitário de Brasília – UniCEUB.

1 INTRODUÇÃO

A globalização trouxe consigo a tecnologia revolucionária, aquela capaz de facilitar a vida das pessoas para realização de atividades cotidianas que seria necessário o deslocamento de lugar e lugar, porém, um simples acesso ao computador, tablet e até mesmo o celular, é capaz de resolver certas situações em um "click". Com a popularização do uso da informática, a consolidação dos dados e das informações pessoais ou públicas se tornaram ferramentas poderosas e eficazes para resultados positivos e resolução de qualquer coisa.

O crescimento espantoso do uso das informações se tornou alvo de reflexão sobre a visão jurídica social, tendo em vista o aspecto criminal das ações praticadas, cujos reflexos são online ou offline, quando da utilização da informática, conhecendo o Direito como o início do ordenamento jurídico que rege e regulamenta as regras gerais da ordem pública e social que prezam pelos princípios da moral e da ética.

Os primeiros crimes virtuais surgiram nos anos 1960, durante a Guerra Fria (EUA contra União Soviética), permitindo somente as forças de segurança o seu uso. No ano de 1970 começaram os acessos aos sistemas privados e ao cometimento de crimes virtuais, como a invasão de sistemas e o roubo de software.

No Brasil a internet surgiu a partir da década de 90 e foi disponibilizada apenas para pesquisas, para algumas universidades, a mesma poderia ser utilizada somente para esse fim. A internet somente começou a ser comercializada uns anos mais tarde, em meados de 1994 começou a ser vendida pela empresa de telecomunicação Embratel. Em 1995 o ministério das telecomunicações em conjunto com o Ministério da Ciência e

Tecnologia, começaram atividades para disponibilizar acesso à internet para a população brasileira.

Em 2018, o Brasil era o segundo colocado no ranking de países com maior número de crimes cibernéticos, perdendo somente para a China.

No final de 2019, o Brasil iniciou a adesão a Convenção de Budapeste, cuja permissão ao Brasil seria o acesso mais rápido a provas eletrônicas que estejam no exterior, mediante cooperação jurídica internacional. A convenção é composta pelos países da União Europeia, Estados Unidos, Japão, Canadá, Chile, Argentina, Austrália, Paraguai e República Dominicana.

Com a facilidade de acesso ao meio digital, a pratica de delitos através do uso da internet se tornou preocupante, pois, a dificuldade de localizar, e em tempo hábil, a pessoa que cometeu tal ocorrência é complicado, uma vez que, agora, mesmo uma pessoa sem conhecimento técnico pode cometer um delito no ciberespaço.

Sendo as regras do direito, o protetor do bem individual e/ou coletivo, público ou privado, aquelas que devem ser cumpridas, tornou-se necessária a ação conjunta dos poderes público e jurídico para ações mais enérgicas contra as infrações em virtude do aumento de casos desses crimes e das novas modalidades de delitos informáticos, assim, surgiram as leis como a do Marco Civil da Internet (Lei Nº 12.965/14), criada em abril de 2014 lei que visa orientar os direitos e deveres dos usuários, provedores de serviços e conteúdos e demais envolvidos com o uso da Internet no Brasil, já a lei Carolina Dieckmann (Lei Nº 12.737/12), criada em novembro de 2012, que promoveu alterações no código penal brasileiro, tipificando os chamados delitos ou crimes informáticos,

considerada um dos primeiros esforços no sentido de estabelecer segurança jurídica para a vida privada online.

Diante dessa breve explicação sobre os crimes cibernéticos, o artigo busca esclarecer e conceituar os crimes próprios e impróprios cometidos através do meio virtual, bem como, o tratamento para coibir essas práticas, pela legislação jurídica atual.

2 SOCIEDADE DA INFORMAÇÃO

A enciclopédia livre Wikipédia, explica que, o termo sociedade da informação, sociedade do conhecimento ou nova economia, teve origem no termo Globalização após a era industrial, surgindo definitivamente no final do século XX, onde a informação se tornou uma ferramenta de fácil acesso e essencial para o desenvolvimento pessoal e coletivo, com o objetivo promover a inovação tecnológica.[2]

O trabalho traz uma explicação de grande relevância, ao afirmar que a sociedade está estruturada e constituída em torno da rede de informação tecnológica, do e-commerce, mudando as relações sociais paulatinamente, vista como um meio muito importante de organização da sociedade, senão, o coração do desenvolvimento social que adveio das mudanças históricas, e que, torna impossível manter a ordem do meio em que vivemos, se não houver essa base material.[3]

Os autores ainda complementam que, os benefícios trazidos são inquestionáveis, porém, sua evolução abrupta acompanhou em passos lentos os riscos de segurança, tanto de pessoas como de

[2] Sociedade da Informação. Disponível em: https://pt.wikipedia.org/wiki/Sociedade_da_informação. Acesso em: 03/06/2020.

[3] BINICHESKI, Paulo Roberto. MARTINS, Plínio Lacerda. A Internet das Coisas e do Sistema Jurídico Brasileiro: Noções Preliminares de responsabilidade Civil Impostas aos Fornecedores de Produtos e Serviços. ***Revista de Direito: Trabalho, Sociedade e Cidadania***. Brasília, v.6, n.6, jan./jun., 2019.

instalações físicas utilizadas, da violação da privacidade e da exposição de dados, entre tantos outros riscos.

3 DEFINIÇÃO DE CRIMES VIRTUAIS

Primeiramente, pode-se conceituar a palavra crime virtual, como a conduta típica, antijurídica e culpável, porém, com o auxílio ou contra os sistemas informatizados. Numa pesquisa realizada pela OECD – Organization for Economic Cooperation and Development (Organização para a Cooperação Econômica e Desenvolvimento) da ONU, a organização define os crimes virtuais como qualquer comportamento ilegal, aético, ou não autorizado envolvendo processamento automático de dados e, ou transmissão de dados.[4]

Um conceito mais detalhado, claro e preciso sobre "delito informático", é o que considera o crime cometido por meio virtual pode ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança da informação e de dados, que tem por elementos a integridade, a disponibilidade a confidencialidade, embora o crime pudesse ser praticado de outra forma, são condutas transgressoras de princípios morais e éticos face ao dinamismo da tecnologia, cujos agentes ativos e passivos, são os usuários do meio virtual (computadores, internet, celulares, etc).[5]

[4] VirtuaJus, Belo Horizonte, v. 2, n. 2, p.338-362, 1º sem. 2017. ISSN - 1678-3425
[5] ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal.** São Paulo: Memória Jurídica, 2004.

Os crimes cibernéticos, são definidos claramente como atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador, que incluem infrações contra o patrimônio, contra a liberdade individual e contra a propriedade imaterial.[6]

3.1 Classificação de crimes virtuais

Com o surgimento de novas modalidades de crimes virtuais, houve também a necessidade de classifica-los com o intuito de compreender melhor esses delitos, pois, as definições criadas anteriormente, ficaram obsoletas por causa da rápida evolução dessa modalidade de infração. Por vários anos, as condutas delituosas que ocorriam na internet com intuito de roubar, ofender, acarretar danos psicológicos, físicos ou financeiros, eram crimes realizados a um indivíduo, órgãos públicos ou a empresas privadas, já essas novas condutas diferem dos crimes praticados no computador, pois não envolvem, na maioria dos casos, os softwares e precisam apenas da internet para acontecer e atingir o objetivo final, mesmo que seja somente uma conversa com uma pessoa para então praticar o crime, como a difamação, a calúnia e/ou a injúria, assim também como, as ameaças e estelionato, esses novos tipos de delitos virtuais são classificados em: crimes virtuais impróprios, crimes virtuais próprios, crimes virtuais indiretos e crimes mistos.[7]

[65] FERREIRA, Ivette Senise. **Direito e Internet: Aspectos jurídicos relevantes**. 2 ed. São Paulo: QuartierLatin, 2005.

[7] VIANA, André de Paula. Crimes virtuais e a necessidade de uma legislação especifica Conteúdo Jurídico, Brasilia-DF:https://conteudojuridico.com.br/consulta/Artigos/49970/crimes-virtuais-e-a-necessidade-de-uma-legislacao-espeficica, 2017. Acesso em 27/05/2020.

O presente artigo abordará sobre os crimes próprios e impróprios, tema desse trabalho acadêmico.

3.2 Crimes virtuais próprios

Os crimes praticados exclusivamente por meio do computador, do sistema informatizado do sujeito passivo, quando utilizado como objeto e meio para invadir dados não autorizados e interferir em dados informatizados, ou seja, são aqueles que, cometidos, causam prejuízos de bens protegidos pela norma penal, sendo inviolável as informações automatizadas (dados), concluindo-se assim, que a segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos, é o objeto jurídico tutelado. Para caracterizar crime próprio virtual, a prática deve ocorrer por meio de uso do computador, bem como, a conclusão, consumação do delito ocorrer também por meio eletrônico.[8]

Podemos citar como exemplo, o caso do vírus Melissa, lançado na rede computadorizada por um hacker, que em 1999 causando um prejuízo de mais de US$ 80.000.000,00 (oitenta milhões de dólares) americanos, outro caso foi em 2011, o furto de dados, nomes, endereços e alguns detalhes de cartões de crédito de 77 milhões de usuários da PlayStation Network. Importante frisar que, os hackers são especialistas, também, em crimes como o estelionato, a falsidade ideológica e fraudes.

3.3 Crimes virtuais impróprios

Um artigo que aborda um conceito interessante, considera as condutas perpetradas contra outros bens jurídicos, por meio de um

[8] CARDOSO, Adeenele Garcia. https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. 01/04/2012. Acesso em 23/05/2020.

sistema informático, ou seja, aqueles nos quais o computador ou qualquer outro aparelho digital é utilizado como instrumento para a efetivação do crime, crimes já tipificados que agora são cometidos no meio informático, com a utilização de computadores e sistemas informáticos, o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não computacionais ou diversos da informática, aqui a internet é somente a ferramenta, usada como outro meio para a prática e a execução de um crime conceituado, previsto e tipificado na forma legal, utiliza-se o computador, mas não tem prejuízo de qualquer bem.[9]

Podemos dizer que são condutas que violam bens jurídicos tradicionais, não diretamente ligados à tecnologia, porém, utiliza-se esta como meio de execução da violabilidade do bem ora tutelado juridicamente.

Podemos definir, então, que os delitos impróprios que ferem as normas legais, e requerem a atuação das normas legais penais, não apresentam diferenças significativas quanto ao *modus operandi*, ou seja, a maneira pela qual o delito é praticado não se faz necessários conhecimentos técnicos, porém, para a prática de delitos considerados próprios, há a necessidade de conhecimentos específicos de computação.[10]

Após a conceituação dos crimes próprios e impróprios virtuais, constata-se que os crimes de cometidos por meio da

[9] VIANA, André de Paula. Crimes virtuais e a necessidade de uma legislação especifica Conteudo Juridico, Brasilia-DF:https://conteudojuridico.com.br/consulta/Artigos/49970/crimes-virtuais-e-a-necessidade-de-uma-legislacao-especificica, 2017. Acesso em 27/05/2020.

[10] SOARES, Daniel Menah Cury. https://www.migalhas.com.br/depeso/308978/crimes-informaticos-uma-breve-resenha-e-apontamento-de-complicacoes, 2019. Acesso em 26/05/2020.

tecnologia da informação estão cada vez mais ousados, possibilitando a violação de bens jurídicos que não encontram guarida no ordenamento jurídico brasileiro, ainda, há que se frisar também, que, tanto que comete o delito, quanto quem sofre, pode ser sujeito público ou privado.

3.4 Sujeitos de crime virtual

Para que uma determinada ação seja considerada crime, necessário se faz a existência do sujeito ativo e do sujeito passivo, onde, o sujeito ativo é aquele que comete a ação criminosa, e o sujeito passivo é aquele que sofre aquela ação.

No conceito mais detalhado, podemos entender como o sujeito ativo do delito, a pessoa humana que age com o fito de cometer o ilícito penal, e estes podem ser cometidos por uma ou mais pessoas. Já o sujeito passivo, é o indivíduo titular que sofreu a ofensa, seja ele, incapaz, seja pessoa jurídica, podendo ocorrer também, com um ou vários sujeitos.[11]

Tratando-se de crime cometido por meio da informática, a possibilidade de chegar ao criminoso, o sujeito ativo, o especialista rastreia-o através da identificação do número do protocolo de comunicação da internet, conhecido como IP (Internet Protocol), o responsável por endereçar e encaminhar os pacotes que trafegam pela rede mundial de computadores.

Então, quando ocorre a conexão de um computador ou dispositivo similar à internet (como celular, tablet etc.), o endereço de IP (Internet Protocol) é atribuído exclusivamente para aquele internauta. Da mesma forma que dois corpos não ocupam o mesmo lugar no espaço, não existem dois usuários com o mesmo

[11] ROCHA, Fernando Galvão da. **Direito penal: parte geral**. Belo Horizonte: Del Rey, 2007. p. 165.

IP durante a navegação na internet (mesmo dia e hora e fuso horário), independentemente de o endereço IP ser estático ou dinâmico.[12]

As definições que nomeiam os sujeitos que cometem crimes cibernéticos são considerados Hackers, porém, vamos definir aqui que, hackers são aqueles que normalmente modificam softwares, desenvolvendo novas funcionalidades, encontrando falhas em sistemas para empresas, ajudando a corrigi-las, etc, os denominados "White-hats" (chapéus brancos), por serem aqueles que utilizam todo o seu conhecimento para melhorar a segurança, de forma legal, já os Crackers, por outro lado, são os verdadeiros invasores de computadores e de sistemas, sendo até mesmo comparados a terroristas, conhecidos como "Black-hats" (chapéus negros) porque utilizam o conhecimento da informática com propósitos ilícitos.

A classificação que define muito bem um cracker, caracteriza-o como a pessoa que possui grande facilidade de análise, assimilação e compreensão, aplicadas ao trabalho com um computador. Ele sabe perfeitamente (como todos nós sabemos) que nenhum sistema é completamente livre de falhas, e sabe onde procurá-las utilizando técnicas das mais variadas. Cracker: possui tanto conhecimento quanto aos hackers, mas com a diferença de que, para eles, não basta entrar em sistemas, quebrar senhas e descobrir falhas: precisam deixar um aviso de que estiveram por lá. Geralmente são recados malcriados, mas, algumas vezes, podem destruir partes do sistema, ou aniquilar tudo o que veem pela frente. Também são atribuídos aos crackers programas que retiram travas de softwares, bem como os que alteram suas

[12] PISA, Pedro. O que é IP? Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/05/o-que-e-ip.html>. Acesso em: 27 dez. 2016.

características, adicionando, ou modificando, opções, muitas vezes relacionadas à pirataria.[13]

Em complemento, é possível que existam outros sujeitos ativos, haja vista que não é necessário que o criminoso seja um expert em acesso à internet, basta que ele possua acesso a uma rede, e assim, divulgue conteúdos proibidos, como a pornografia infantil, ou também que se aproveite da facilidade do anonimato na internet para cometer crimes contra a honra de outrem.

3.5 Principais crimes virtuais

Os crimes informáticos, não difere em muito dos crimes praticados fora do mundo virtual. Com o avanço da tecnologia, do acesso à informação e dos meios digitais, afim de facilitar a vida de todos, os criminosos se aproveitam da falta de cuidado dos internautas para coletar informações pessoais capazes de acessar qualquer. Assim, lemramos que a gama de delitos que podem ser perpetrados pela Internet é quase infinita. A lista inclui o mau uso dos cartões de crédito, ofensas contra a honra, apologia de crimes, como racismo, ou incentivo ao uso de drogas, ameaças e extorsão, acesso não autorizado a arquivos confidenciais, destruição e falsificação de arquivos, programas copiados ilegalmente e até crime eleitoral (propaganda não autorizada, por exemplo), dentre outros, e um dos crimes mais horríveis, que é pedofilia e a pornografia infantil.[14]

Analisando um estudo geral e breve sobre a pedofilia, o autor aponta que, de acordo com a Classificação Estatística Internacional de Doenças e Problemas Relacionados à Saúde (CID-10), a

[13] OLIVEIRA, Wilson José. Dossiê hacker: técnicas profissionais para conhecer e proteger-se de ataques. São Paulo: Digerati Books, 2006. p. 26.
[14] REIS, Maria Helena Junqueira. Computer crimes: a criminalidade na era dos computadores. Belo Horizonte: Del Rey, 1996. p. 30.

pedofilia é considerada um transtorno mental severo que causa desejos sexuais envolvendo crianças, e por se tratar de um transtorno psiquiátrico, não existe uma tipificação penal para a pessoa que comete a pedofilia, porém, ao exteriorizar e satisfazer seus desejos, o pedófilo comete a lascívia, considerando-se assim, quando envolve menores de 14 anos, o estupro de vulnerável.[15]

Sobre esse assunto, relatamos que a exploração de pornografia infantil se tornou alvo da rede de comunicação internet, com sua transmissão e armazenamento de dados e de informações na velocidade da "luz" para o mundo, facilitando as condutas dos pedófilos em todas as suas formas, haja vista a segurança, de certa forma, do anonimato que a rede propicia. A autora ressalta, ainda, que a pornografia infantil é a divulgação de conteúdo sexual, não necessariamente em atividade sexual, mas, também, divulgação dos órgãos sexuais de uma criança, como dispõe os artigos 241 e 241-A do Estatuto da Criança e do Adolescente.[16]

Em 14 anos, a SaferNet Brasil (Associação Civil voltada para o combate à pornografia infantil na internet brasileira), informa que recebeu e processou 4.134.808 denúncias anônimas, envolvendo 790.390 páginas (URLs) distintas em 9 idiomas e hospedadas em 73.000 domínios diferentes, de 267 diferentes TLDs conectados à Internet através de 71.049 números de IPs distintos, atribuídos para 104 países em 6 continentes, ajudando 30.389 pessoas em 27 unidades da federação, atendendo 8.543

[15] CRESPO, Marcelo Xavier de Freitas. **Revenge porn: a pornografia da vingança. 2014**. Disponível em: <http://marcelocrespo1.jusbrasil.com.br/artigos/153948423/revenge-porn-a-pornografia-da-vinganca>. Acesso em: 27 dez. 2016.

[16] BRITO, Aurinei. **Direito penal informático**. São Paulo: Saraiva, 2013. p. 25.

crianças e adolescentes, 2.180 pais e educadores, 3.471 jovens e 16.195 outros adultos em seu canal de ajuda e orientação.[17]

3.6 Aplicação da legislação brasileira

Ressalta-se que, até o ano de 2012, a legislação punitiva, era aplicada somente aos crimes virtuais impróprios, como exemplos, tem-se: a Lei nº 11.829/2008, de combate a pornografia infantil na internet; a Lei nº 9.609/1998, de proteção da propriedade intelectual de programa de computador; a Lei nº 9.983/2000, que tipifica os crimes de acesso indevido a sistemas informatizados da Administração Pública; a Lei nº 9.296/1996, que disciplina a interceptação de comunicação telemática ou informática e a Lei nº 12.034/2009, que delimita os direitos e deveres durante as campanhas eleitorais e por meio virtual.[18]

Após os ataques distribuídos de negação de serviço a sites do governo e a e a divulgação de fotos íntimas da atriz Carolina Dieckmann, viu-se a necessidade de avançar de forma enérgica com a criação de leis para coibir esses tipos de crimes.

Inicialmente, a PL 84/99 foi transformada na Lei Ordinária 12.735/12, conhecida como "Lei Azeredo", que dispunha sobre os crimes, penas e outras providências cometidos por meio virtual, que alterou somente o inciso II do § 3° do art. 20 da Lei n° 7.716/8918 (Lei do Crime Racial), com o fito de permitir que os conteúdos discriminatório de rádio, TV ou Internet, e de qualquer meio possível, fossem solicitados por um Juiz, e ainda, para combater os crimes cometidos por meio da Internet ou por sistema

[17] Indicadores. Disponível em: https://indicadores.safernet.org.br/indicadores.html. Acesso em: 28/05/2020.

[18] Disponível em: VirtuaJus, Belo Horizonte, v. 2, n. 2, p.338-362, 1º sem. 2017. ISSN - 1678-3425. Acesso em [15] [17] Delitos virtuais praticados na sociedade da informacao/. Disponível em: http://www.rkladvocacia.com/. Acesso em: 30/05/2020.

informatizados, determinava também que polícia judiciária tinham o dever de criar delegacias especializadas para coibir essas práticas delituosas. Também citamos que, antes não existia lei de proteção para o objeto jurídico tutelado da liberdade individual do usuário do dispositivo informático, devido tal "brecha", que ficou amplamente visível com a divulgação de fotos íntimas da atriz Carolina Dieckmann, deu ensejo a sanção urgente das Lei Ordinária, mencionada anteriormente e a Lei 12.737/2012, conhecida como "Lei Carolina Dieckmann", afim de proteger os dados ou informações do titular do dispositivo.[19]

Não obstante a essas leis, em 2014, foi sancionada a Lei 12.965/2014 (Marco Civil da Internet), na tentativa de ordenar os parâmetros jurídicos e estabelecendo os princípios, garantias, direitos e deveres que protegem à manifestação do pensamento, à criação, à expressão e à informação por meio do uso virtual, ao mesmo tempo, tutelar o conteúdo da informação e da comunicação social, incluindo os dispositivos constitucionais fundamentais da pessoa humana da vida privada, a proteção à privacidade dos usuários e a garantia de não responsabilização do provedor de internet pela divulgação de conteúdos por terceiros, salvo se, houve determinação judicial anterior que retirassem as informações do meio virtual e o provedor não o fez, assim também, como resguarda o próprio Estado no cumprimento da legislação norteadora do bem comum e social.[20]

[19] Leis Azeredo e Carolina Dieckmann são aprovadas; Marco Civil da Internet corre o risco de sofrer alterações perigosas. Disponível em: https://gizmodo.uol.com.br/. Acesso em: 29/05/2020.

[20] Marco Civil da Internet. Disponível em: https://pt.wikipedia.org/wiki/. Acesso em: 30/05/2020.

REFERÊNCIAS

BINICHESKI, Paulo Roberto. MARTINS, Plínio Lacerda. A Internet das Coisas e do Sistema Jurídico Brasileiro: Noções Preliminares de responsabilidade Civil Impostas aos Fornecedores de Produtos e Serviços. ***Revista de Direito: Trabalho, Sociedade e Cidadania***. Brasília, v.6, n.6, jan./jun., 2019.

BRITO, Aurinei. *Direito penal informático*. São Paulo: Saraiva, 2013. p. 25.

CARDOSO, Adeenele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Disponível em: Acesso em 23/05/2020.

CRESPO, Marcelo Xavier de Freitas. Revenge porn: a pornografia da vingança. 2014. Disponível em: <http://marcelocrespo1.jusbrasil.com.br/artigos/153948423/revenge-porn-a-pornografia-da-vinganca>. Acesso em: 25/05/2020.

Crimes Cibernéticos: Aspectos legislativos e implicações na persecução penal com base nas legislações brasileiras e internacional. Disponível em VirtuaJus, Belo Horizonte, v. 2, n. 2, p.338-362, 1º sem. 2017. ISSN - 1678-3425 Acesso em: 22/05/2020.

Delitos virtuais praticados na sociedade da informação. Disponível em: http://www.rkladvocacia.com/. Acesso em: 22/05/2020.

FERREIRA, Ivette Senise. *Direito e Internet: Aspectos jurídicos relevantes.* 2 ed. São Paulo: QuartierLatin, 2005.

Leis Azeredo e Carolina Dieckmann são aprovadas; Marco Civil da Internet corre o risco de sofrer alterações perigosas. Disponível em: https://gizmodo.uol.com.br/. Acesso em: 29/05/2020.

Marco Civil da Internet. Disponível em: https://pt.wikipedia.org/wiki/. Acesso em: 30/05/2020.

OLIVEIRA, Wilson José. *Dossiê hacker: técnicas profissionais para conhecer e proteger-se de ataques*. São Paulo: Digerati Books, 2006. p. 26.

PISA, Pedro. O que é IP? Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/05/o-que-e-ip.html>. Acesso em: 23/05/2020.

REIS, Maria Helena Junqueira. *Computer crimes: a criminalidade na era dos computadores.* Belo Horizonte: Del Rey, 1996. p. 30.

ROSSINI, Augusto Eduardo de Souza. *Informática, telemática e direito penal*. São Paulo: Memória Jurídica, 2004.

ROCHA, Fernando Galvão da. *Direito penal: parte geral.* Belo Horizonte: Del Rey, 2007. p. 165.

SOARES, Daniel Menah Cury. Crimes informaticos uma breve resenha e apontamento de complicacoes. Disponível em: https://www.migalhas.com.br/depeso/308978/ crimes-informaticos-uma-breve-resenha-e-apontamento-de-complicacoes, 2019. Acesso em 26/05/2020.

VIANNA, Túlio Lima. Fundamentos de Direito Penal Informático: do acesso não autorizado a sistemas computacionais. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2003;000640215. Acesso em: 27/05/2020.

VIANA, André de Paula. Crimes virtuais e a necessidade de uma legislação específica Conteúdo Jurídico, Brasília-DF: Disponível em: https://conteudojuridico.com.br/consulta/Artigos/49970/crimes-virtuais-e-a-necessidade-de-uma-legislacao-espeficica, 2017. Acesso em 27/05/2020.

Safernet-Indicadores. Disponível em: https://indicadores.safernet.org.br/indicadores.html. Acesso em: 24/05/2020.

Sociedade da Informação. Disponível em: https://pt.wikipedia.org/wiki/Sociedade_da_informação. Acesso em: 03/06/2020.

CIBERCRIME: UMA BREVE ANÁLISE DOS SUJEITOS E PRINCIPAIS DELITOS VIRTUAIS

Karl Heisenber Ferro Santos[1]

RESUMO

Este artigo propõe uma reflexão sobre os sujeitos e os principais delitos virtuais que se encontram no âmbito dos crimes virtuais. Diante disso, faz-se imprescindível o exame de aspectos conceituais e classificatórios, com a finalidade de se atingir e assimilar os principais atores e os delitos mais frequentes. Explanar e identificar as propriedades e as peculiaridades, como também os polos presentes na relação são pontos cruciais para o desenvolvimento deste trabalho. Justifica-se, ainda, a importância deste artigo, já que os crimes cibernéticos são cada vez mais comuns no dia a dia do cidadão.

Palavras-chave: Crimes Virtuais. Sujeitos. Delitos.

ABSTRACT

This article proposes a reflection on the subjects and the main virtual crimes that are within the scope of virtual crimes. Given this, it is essential to examine conceptual and classificatory aspects, in order to reach and assimilate the main actors and the most frequent crimes. Explaining and identifying the properties and peculiarities, as well as the poles present in the relationship, are crucial points for the development of this work. The importance of this article is also justified, since cyber crimes are increasingly common in the daily lives of citizens.

Keywords: Virtual Crimes. Subjects. Offenses.

[1] Aluno da Pós Graduação *lato sensu* em Direito do Instituto Ceub de Pesquisa e Desenvolvimento – ICPD – do Centro Universitário de Brasília – UniCEUB.

1 INTRODUÇÃO

As novas tecnologias já fazem parte do quotidiano do ser humano. O uso constante e exagerado da internet é o principal motivo pelo qual denominamos a sociedade atual como a sociedade da informação.

O espaço virtual tem servido a um novo tipo de criminalidade, dado que a probabilidade de impunidade, na execução de novos crimes e delitos são muitas vezes enxergados. A criminalidade informática não se limitará aos crimes que englobem o elemento digital como parte formadora do seu tipo legal ou matéria de proteção, mas se estende a todo o tipo de infração praticada por meio informático.

O primeiro item do presente artigo é para situar e dar melhor entendimento, pois a conceituação e a qualificação das condutas são pedras basilares quando tratamos dos crimes cibernéticos. É notório que existe uma vasta concepção sobre os crimes que acontecem na rede mundial de computadores. Todavia, a sua natureza resume-se ao meio empregado, quer seja a internet ou ferramentas que a utilize.

No item 2 do presente artigo, é a conceituação e a qualificação das condutas são basilares quando tratamos dos crimes cibernéticos. Eles podem ser divididos em crimes próprios, que condutas perpetradas contra um sistema informático, sejam quais forem as motivações do agente e crimes e impróprios, aqueles efetuados contra outros bens jurídicos, por meio de um sistema informático.

Em seguida, no item 3, aborda-se a dificuldade existente, por parte das autoridades, na identificação dos sujeitos ativos dos crimes cibernéticos. Na verdade, existe uma separação, ou seja,

sujeitos ativos são aqueles que praticam a ação ilícita através de diferentes equipamentos tecnológicos, dentre estes, os hackers, os crackers e os lammers. E de outro, sujeito passivo é o aquele que sofre o crime, a vítima do delito, que tem sua propriedade transgredida, podendo ser pessoa física ou pessoa jurídica, ou até mesmo instituição pública ou privada.

Por fim, modernas condutas sociais são originadas diariamente, e com isso novos tipos penais surgem nos ordenamentos jurídicos. Proporcionar e assegurar a segurança jurídica são desafios constantes no mundo do direito. Os crimes contra a honra, do estelionato e da invasão de dispositivos informáticos, são apenas alguns exemplos de delitos, que estão ganhando, gradativamente, um espaço no campo virtual.

2 CIBERCRIME: CONCEITO E CLASSIFICAÇÃO DAS CONDUTAS

2.1 Conceito

Josefa Cristina Kunrath, (2017, p.45) afirma que "os ilícitos, através das redes telemáticas (internet) assumem várias nomenclaturas, tais como cibercrime, crime digital, crime informático, crime informático digital, cybercrime, crimes eletrônicos, delitos de computador, delitos computacionais, crime de computação, etc."

Diante disso, é forçoso entender que todas as definições acima transcritas serão utilizadas no discorrer deste artigo, evitando, assim, a repetição de palavras.

Em harmonia com o art. 1º da Lei de introdução do Código Penal:

> Art. 1º Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente.

Nessa continuação, "os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados", segundo o preâmbulo da Convenção de Budapeste sobre o Cibercrime (2001).

O escritor, Sérgio Marcos Roque (2007, p.25) conceitua crime cibernético como "toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material".

Por sua vez, Augusto Rossini, aduz:

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

A advogada e escritora, Ivette Senise Ferreira, classifica da seguinte maneira:

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

Se respeitarmos a classificação definida por Fabrizio Rosa (2002, p.53-54), verifica-se que o procedimento que vai contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela seleção, retenção ou divulgação de dados, depreendida pelos fundamentos que formam um sistema de tratamento, seja ainda, na forma mais rudimentar. O crime digital dá a entender que os elementos são indissolúveis, pois atentam contra os dados que estejam preparados às operações do computador e, também, por meio do computador, utilizando-se software e hardware, para perpetrá-los.

Perceba, que os e-crimes é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento eletrônico de dados ou seu compartilhamento. A ação típica é a aplicação de um sistema informático que serve para cometer uma ação contra um bem ou interesse juridicamente protegido, esteja ele ligado à ordem econômica, à integridade física, à liberdade do cidadão, à privacidade, à honra ou até mesmo à Administração Pública.

Portanto, é perceptível que existe uma vasta conceituação de crimes na rede mundial de computadores. Todavia, a sua natureza resume-se ao meio empregado, quer seja a internet ou ferramentas que a utilize.

2.2 Classificação das Condutas

Na esfera dos crimes digitais, ainda existem áreas de grande complexidade. Os desentendimentos doutrinários se fazem presentes na maioria dos debates. Contudo, para um melhor entendimento e de forma mais simples, este presente artigo concorda com o raciocínio do professor Vicente Greco Filho, que explica:

Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da Internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou. (GRECO, 2000, p.3)

Em resumo, os crimes cibernéticos podem ser divididos em crimes próprios, que condutas perpetradas contra um sistema informático, sejam quais forem as motivações do agente e crimes e impróprios, aqueles efetuados contra outros bens jurídicos, por meio de um sistema informático.

2.3 Crimes Virtuais Puros ou Próprios

A principal característica do crime virtual próprio é a necessidade do sujeito passivo em utilizar o sistema informático como objeto e meio do crime praticado.

No mesmo sentido, Maria Castro de Almeida afirma:

> Os crimes próprios, também chamados de crimes puros são aqueles que só podem ser praticados na informática, ou seja, a execução e a consumação ocorrem nesse meio. Tratam-se de tipos novos em que o bem jurídico tutelado é a informática. São aqueles em que o sujeito se utiliza necessariamente do computador, que é

> usado como objeto e meio para execução do crime. (DE ALMEIDA, 2015, p.6)

Crime cibernético puro, para Marco Túlio Viana (2003, p. 13), "são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados). "

O doutrinador, Damásio de Jesus, constata como:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. (JESUS, 2003 apud CARNEIRO, 2012).

Portanto, nesta divisão de crimes se insere a invasão de dados armazenados em computador, objetivando a modificação, alteração ou a inserção de dados falsos, por meio de software ou hardware do dispositivo e somente podem ser concretizados pelo computador ou contra ele e seus periféricos. O bem jurídico protegido, neste caso, pela norma penal é a interceptação telemática ilegal, a violação de e-mail, o dano em arquivos causado pelo envio de vírus, entre outros.

2.4 Crimes Virtuais Abertos ou Impróprios

Por sua vez, os crimes cibernéticos denominados de abertos ou impróprios já estão devidamente tipificados pelo Direito Penal, porém são executados com a utilização de dispositivos ou da rede de computadores, isto é, a própria máquina em si é manuseada como meio para a realização dos atos inflacionários e ilícitos. Logo, são aqueles já presentes e que ferem bens normalmente protegidos pela legislação pátria, podendo ser praticados de qualquer maneira, sendo o computador ou notebook apenas um modo de execução.

O professor, Marcelo Xavier de Freitas Crespo, reconhece:

os crimes digitais impróprios nada mais são que aqueles já tradicionalmente tipificados no ordenamento, mas agora praticados com auxílio de modernas tecnologias. Assim, essa denominação apenas representa que os ilícitos penais tradicionais podem ser cometidos por meio de novos *modi operandi*. (CRESPO, 2011, p.95)

Assim entende DAMÁSIO:

> [...] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática. (JESUS, 2003 apud CARNEIRO, 2012).

Exemplos de crimes virtuais impróprios, entre outras muitas, englobam, também, as violações praticadas contra a honra do indivíduo, elencados nos artigos 138, 139 e 140 do Código Penal. São, respectivamente: calúnia, difamação e injúria.

Para se compreender e categorizar alguns crimes a didática se faz imprescindível. A velocidade e rapidez dos acontecimentos no mundo virtual torna quase impossível acompanhar e aduzir que não existam modalidades que não estejam elencadas nas classificações adotadas.

3 DOS SUJEITOS

A jurisdição brasileira sente enorme dificuldade em identificar os sujeitos ativos dos crimes virtuais, uma vez que a quantidade de usuários é cada vez maior. Nota-se, então, que o responsável pela infração é conhecedor de técnicas especializadas e amplo entendedor do mundo informático, o que facilita a ação.

Similarmente às classificações das condutas, no quesito dos sujeitos, também, subsiste uma fragmentação entre os personagens. O sujeito ativo é quem pratica a ação ilícita através de diferentes equipamentos tecnológicos, dentre estes, os hackers, os crackers, os lammers, e outros que veremos a seguir. Por outro lado, o sujeito passivo é o cidadão que sofre o crime, a vítima do delito, que tem sua propriedade transgredida, podendo ser pessoa física ou pessoa jurídica, ou até mesmo instituição pública ou privada.

3.1 Sujeitos Ativos

É bastante comum que quando se trata de delitos virtuais, a sociedade tenha a ideia de que tais práticas sejam realizadas apenas por profissionais ou *experts*, isto é, os sujeitos ativos mais conhecidos como *Hackers* ou *Crackers.* Todavia, a globalização tem cooperado enormemente na popularização dos sistemas de informação, o que tem provocado uma nova onda de crimes virtuais por aqueles que não possuem um domínio tecnológico aprofundado.

Os crimes com tendências difamatórias, vexatórias, sexuais e racistas se fazem presente no dia a dia do cidadão brasileiro. A facilidade de comunicação e propagação de mensagens por meio de aplicativos torna possível que qualquer indivíduo seja um sujeito ativo de crimes virtuais, pois só estar conectado à internet é o suficiente.

Portanto, para uma melhor compreensão dos diferentes tipos de sujeitos ativos, se faz mister uma explanação de cada ator que se encontra no polo ativo dos crimes eletrônicos. Ora vejamos:

3.2 Hackers

Os principais "piratas" da computação são conhecidos como Hackers. Os estudantes do instituto de tecnologia de Massachussetts foram os responsáveis por tal denominação, já que viravam noites "caçando novos tesouros" nos computadores dos laboratórios.

Em sua obra, Marcelo Crespo (2011, p.106) alega que "a melhor tradução para referida expressão inglesa é "fuçador", e que "a tal palavra é no sentido daquele que invade sistemas em benefício próprio, obtendo dados e informações alheias (documentos, programas, músicas etc.), mas sem danificar nada. "

O escritor, Wilson José de Oliveira (2006, p.26), explica que o Hacker é um sujeito dotado de amplo conhecimento técnico no mundo informático, pois entende que nenhum sistema é completamente perfeito, e isso o estimula a cometer delitos. Já os Crackers, possuem o mesmo conhecimento que os Hackers, todavia, não basta entrar em sistemas, quebrar senhas e descobrir falhas, é necessário tornar público o ato realizado, isto é, gostam de um certo protagonismo e celebram a ação executada. Normalmente são recados ofensivos, ou em outras, a própria destruição de partes do sistema.

O escritor Moisés de Oliveira Cassanti declara:

> O termo hacker, por sua vez, serve para designar um programador com amplo conhecimento sobre sistemas, mas sem a intenção de causar danos. Inclusive, a habilidade para lidar com sistemas e programações, muitas vezes, é aplicada pela própria polícia em investigações ou até mesmo no desenvolvimento de softwares com o intuito de limar brechas de segurança, criar novas funcionalidades ou adaptar as antigas. (CASSANTI, 2014, p.19-20)

3.3 Crackers

No que diz respeito aos Crackers, Marcelo Crespo define:

> O cracker é aquele que, basicamente, "quebra" um sistema de segurança, invadindo-o. Fanáticos pelo vandalismo, também adoram "pichar" páginas da web deixando, na maioria das vezes, mensagens de conteúdo ofensivo e racista. Vale frisar que geralmente os criminosos da informática são mesmo os crackers, embora não sejam os únicos. A expressão consagrada, porém, para criminosos que utilizam computadores como arma é hacker. (CRESPO, 2011, p.106)

Em seu blog, a faculdade Unyleya estabelece que os crackers "são indivíduos que possuem um conhecimento elevado na área de tecnologia da informação, mas que utilizam suas habilidades em benefício próprio ou para prejudicar outras empresas e pessoas. "

Um dos maiores sites de informática no Brasil, o canaltech delibera:

> Diferentemente do que muitas pessoas podem pensar, quem utiliza os seus conhecimentos de informática para coletar informações, descobrir senhas de acesso a redes e quebrar códigos de segurança em benefício próprio, não são os hackers. Os responsáveis por tais práticas criminosas, na verdade, são os crackers. Embora esse segundo nome não seja tão difundido quanto o primeiro, ele é o correto para se utilizar ao designar alguém que contraria a lei e age sempre em benefício próprio ao cometer delitos virtuais. Os crackers costumam quebrar códigos de seguranças de programas, o que faz com que eles se tornem "crackeados". Já o termo "crack" é usado para se referir a alguma ferramenta (como aplicativos, links e programas) utilizada por crackers para obter acesso a chaves de registro e licenças de produtos pagos.

3.4 Carders

Por seu turno, Crespo (2011) define os Carders como sendo estelionatários específicos, pois a sua denominação provém do fato de realizarem compras virtuais por meio de cartões de créditos de terceiros. Os computadores das administradoras de cartões de créditos começam por ser atacados, os números são subtraídos, e logo após ocorre a repartição para que uma quantidade maior de pessoas tenha acesso e isso torna mais difícil encontrar quem os subtraiu.

Nessa continuação vai o entendimento de Moisés de Oliveira Cassanti:

> especialista em roubar informações bancárias como números de cartões de crédito, cartões de conta corrente ou poupança, ou contas em sites de movimentações bancárias, para compras on-line, saques em caixas eletrônicos, transferência para contas de laranjas entre outros atos ilícitos. (CASSANTI, 2014, p.20)

3.5 Lammers

O site canaltech define: "Lammer ou Lamer é um termo utilizado para as pessoas que não possuem nenhum ou pouco conhecimento sobre hack e utilizam ferramentas desenvolvidas por outros para realizarem seus ataques. "

De forma mais detalhada, o Instituto Information Management elucida que os Lammers "São aqueles "*crackers*" inexperientes que atuam na realização de algum tipo de ação dentro do universo de segurança da informação, mas têm pouca ou quase nenhuma experiência. "

Continuam elucidando que "atuam de forma totalmente amadora, através de experiências feitas por crackers com o intuito

de utilizar-se das técnicas existentes para competir por reputação e reconhecimento. ”

3.6 Wannabes

Os *Wannabes*, são pessoas que desejam ser *Hackers*, porém ainda não atingiram esse feito. A despeito de terem certo conhecimento informático, não detêm a mesma habilidade, pois este é a apreensão de Marcelo Crespo:

São assim chamados porque querem ser especialistas, mas não são. São pessoas que já aprenderam um pouco sobre hacking e não estão aptos a praticar grandes feitos. Apesar disso, já fazem o que aprenderam com competência. Diferenciam-se dos lammers por terem mais consciência do que são capazes de fazer. (CRESPO, 2011, p.108)

3.7 Phreakers

Por fim, os *Phreakers*, de acordo com Moisés Cassanti (2014, p.20), é um “especialista que utiliza técnicas para burlar os sistemas de segurança das companhias telefônicas, normalmente para fazer ligações de graça ou conseguir créditos. ”

De forma similar, Marcelo Crespo (2011, p.108) entende que os *Phreakers* são os especialistas em telefonia, uma vez que usam a sua inteligência para realizar ligações gratuitas ou escutas telefônicas. Estas últimas são usadas em computadores e, no momento em que um telefone toca, o do *Phreacker* também o faz, pois, assim, ele escuta conversas alheias. Entretanto, não se limitam a isso, já que são capazes de fazer ligações sem que nenhum tipo de pagamento seja realizado, sendo que ocorre uma confusão quanto à origem da ligação e quem paga a conta é qualquer outra pessoa que tenha telefone daquela operadora.

3.8 Sujeito Passivo

No momento em que falamos de crime é intrínseco que exista um polo ativo e passivo da conduta, ou seja, quem praticou ato ilícito e quem é o titular do bem lesado ou ameaçado pela conduta criminosa.

Júlio Fabrinni Mirabete (2008, p. 114), enfatiza que "o sujeito passivo podem ser duas ou mais vítimas, como estabelecido no artigo 147 do Código Penal: "ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave", esse crime é comum nas redes virtuais, podendo ter ao mesmo tempo duas ou mais vítimas. "

Entende-se, então, que o sujeito passivo da infração penal pode ser qualquer cidadão, pessoa física ou até mesmo uma pessoa jurídica, dado que prática muito comum nos crimes virtuais contra instituições ou empresas são os desvios de dinheiro, a deterioração de patrimônio ou a violação e roubo de informações.

Acontece, que empresas nacionais e multinacionais têm evitado a divulgação de ataques virtuais, pois entendem que essa publicidade poderia prejudicar a sua imagem e demonstrar fragilidade em relação à segurança, o que ocasionaria na perda de investidores e confiança de mercado. Em contrapartida, o cidadão comum, pessoa física, neste caso, visualiza a falta de punibilidade e de mecanismos de acusação, os fatores mais relevantes para não levarem adiante a devida denúncia, o que favorece o crescimento e a multiplicação desses crimes.

Constata-se, que qualquer ser humano está propício a ser vítima e se tornar sujeito passivo de e-crimes, visto que a capacitação e o profissionalismo, por parte dos criminosos, são

cada vez maiores, aliados às novas tendências tecnológicas, alcançando, desse jeito, a maior parte da população.

4 PRINCIPAIS DELITOS VIRTUAIS

O surgimento da internet e a consequente criação de diferentes tipos de redes sociais, fez com que as pessoas se relacionassem e interagissem em uma maior proporção.

Nesse contexto, surgiram novas práticas, a criação de perfis falsos, os discursos de ódio, a invasão de privacidade, o compartilhamento de vídeos pessoais e o furto de dados demonstram que a esfera criminal e o mundo digital têm dialogado cada vez mais.

À medida que o corpo social tem tido mais facilidade em acessar e utilizar a *world wide web*, também é fabricado inúmeros instrumentos para o cometimento de crimes eletrônicos.

Neste instante, a preocupação em proteger os dados dos cidadãos e ao mesmo tempo reprimir e penalizar os cibercrimes, são as maiores preocupações das instituições e empresas que atuam no campo cibernético, tanto na defesa como na persecução penal.

Os crimes contra a honra, o estelionato e a invasão de dispositivos, são apenas alguns exemplos de delitos, que estão ganhando, gradativamente, um espaço no campo virtual.

4.1 Crimes contra a honra

Constantemente praticados na internet, com maior ênfase nas redes sociais, os crimes contra a honra estão presentes no Capítulo V, do Código Penal.

Por isso, e de forma preliminar, é preciso conhecer o conceito de honra. O doutrinador e jurista, Luiz Regis Prado, conceitua da seguinte forma:

> "[...] a honra, do ponto de vista objetivo, seria a reputação que o indivíduo desfruta em determinado meio social, a estima que lhe é conferida; subjetivamente, a honra seria o sentimento da própria dignidade ou decoro. A calúnia e a difamação atingiriam a honra no sentido objetivo (reputação, estima social, bom nome); já a injúria ofenderia a honra subjetiva (dignidade, decoro). " (PRADO, 2008, p. 213)

Na esfera constitucional, a tutela ao bem jurídico da honra, se encontra no art. 5º, inciso X, da Carta Magna "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".

Em relação ao Código Penal brasileiro, encontramos três tipos penais que protegem a honra do cidadão, a saber: calúnia (art. 138), a difamação (art. 139) e a injúria (art. 140).

4.2 Calúnia

A calúnia é o mais grave de todos os crimes contra a honra previstos no Código Penal. Em sua conduta típica, a lei penal aduz expressamente à imputação falsa de um fato definido como crime.

Está previsto no art. 138 do Código Penal que "caluniar alguém, imputando-lhe falsamente fato definido como crime", é cabível pena de detenção de seis meses a dois anos e multa. Há calúnia também quando alguém, conhecendo a falsidade, propala ou divulga a imputação (§ 1º). Punível, igualmente, a calúnia contra os mortos (§ 2º).

Consoante Rogério Greco:

> podemos indicar os três pontos principais que especializam a calúnia com relação às demais infrações penais contra a honra, a saber: o primeiro é a imputação de um fato; o segundo esse fato imputado à vítima deve, obrigatoriamente, ser falso; o terceiro além de falso, o fato deve ser definido como crime. (GRECO, 2016, p.418)

Resta comprovado, que a conduta do crime de calúnia se enquadra perfeitamente no mundo virtual. Importante destacar, que, também, será imputado àquele que divulga ou propala a falsa imputação, algo bem corrente na sociedade contemporânea, de acordo com o §1º do art. 138, do CP.

4.3 Difamação

Relativamente ao crime de difamação, a vítima tem sua honra atingida pela imputação de fato que não é crime, podendo ser uma contravenção penal ou fato atípico para o direito penal brasileiro.

O professor Rogério Greco (2016, p.428), ensina que "Para que se configure a difamação deve existir uma imputação de fatos determinados, sejam eles falsos ou verdadeiros, à pessoa determinada ou mesmo a pessoas também determinadas, que tenha por finalidade macular a sua reputação, vale dizer, sua honra objetiva. "

É imprescindível, que no crime de difamação, o sujeito ativo tenha o animus *diffamandi*, ou seja, o agressor deve ter a intenção e a consciência de imputar fato a terceiro com o intuito de ofender sua honra. Caso não exista essa consciência, a difamação não será configurada.

A divulgação de fotos ou vídeos, eróticos ou pornográficos, é uma prática cada vez mais comum entre casais. É chamada de

sexting, que é o envio de mensagens com conteúdo íntimo e sexual a um indivíduo, porém, que se torna um crime se essa pessoa que recebe a mensagem, a repassa sem o consentimento de quem a enviou.

Carolina Tanaka explica:

> É nesse tipo penal que se enquadra a pornografia de vingança e a divulgação não consentida do *sexting*, pois, ofendem a honra objetiva da vítima tendo em vista que a exposição da sexualidade da mulher é vista como um tabu e com maus olhos pela sociedade, que julgam e desaprovam esse tipo de conduta. (TANAKA, 2016, p.9)

Depreende-se, que a pornografia da vingança se adequa perfeitamente ao art. 139, do CP; difamação: "Difamar alguém, imputando-lhe fato ofensivo à sua reputação. " É, sem sombra de dúvidas, um fato ofensivo à reputação da vítima, uma vez que expõe a sua intimidade perante pessoas que não faziam parte do relacionamento.

4.4 Injúria

O derradeiro crime contra a honra é o crime de Injúria. Este tipo penal está descrito no artigo 140 do Código Penal vigente, que tem a redação:

> 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.
>
> § 3] 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: (Redação dada pela Lei nº 10.741, de 2003)
>
> Pena - reclusão de um a três anos e multa

Desta forma, Rogério Greco nos ensina sobre o tema:

> De todas as infrações penais tipificadas no Código Penal que visam proteger a honra, a injúria, na sua modalidade fundamental, é a considerada menos grave. Entretanto, por mais paradoxal que possa parecer, a injúria se transforma na mais grave infração penal contra a honra quando consiste na utilização de elementos referentes à raça, cor, etnia, religião, origem ou à condição de pessoa idosa, ou portadora de deficiência, sendo denominada, aqui, de injúria preconceituosa (...) (GRECO, 2016, p.433)

E continua explicando (GRECO, 2016, p.433) "já a injúria se difere dos outros crimes contra a honra, pois tutela a honra subjetiva do indivíduo, ou seja, a autoestima da pessoa, e como ela mesma vê seus atributos físicos, morais ou intelectuais".

A ofensa, neste caso, é direcionada à dignidade ou autoestima de um indivíduo. É uma prática muito comum em ambiente virtual, pois, o sujeito ativo se utiliza do anonimato e da forte possibilidade de apagar e deletar as ações e conteúdos ofensivos, que de forma virtual se torna mais cômodo em praticar atos ilícitos.

Pelo ensinamento de Rogério Greco, citado acima, percebe-se que se trata de um crime que pode ser realizado de forma livre, então isso acaba se mostrando muito comum em redes sociais ou sites que divulgam imagens, frases, ou qualquer conteúdo que atribuam qualidades negativas a alguém, sendo muito comum injúria racial ou por qualquer tipo de preconceito.

4.5 Estelionato Digital

A crise econômica, o isolamento social e o avanço tecnológico, acrescido à pouca informação e instrução da população no que toca à utilização dos dispositivos que utilizam a internet, fazem com que haja um forte crescimento de sujeitos passivos nos crimes eletrônicos.

Os cibercriminosos aproveitam-se do momento atual, com o intuito de ludibriar os menos informados, elaboraram novas estratégias, técnicas e métodos para a realização de crimes. O crescimento do comércio eletrônico, as oportunidades de bons negócios, os descontos avassaladores, são a isca perfeita para a obtenção de vantagens indevidas.

Assim surgem os estelionatos digitais.

É bem verdade que não existe uma lei específica para essa conduta, todavia, o crime de estelionato, se faz presente no artigo 171 do Código Penal: "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento".

Rogério Grego (2009, p.228), afirma que: "desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas"

Julio Fabbrini Mirabete (2008, p.287), entende que: "Existe o crime, portanto, quando o agente emprega qualquer meio fraudulento, induzindo alguém em erro ou mantendo-o nessa situação e conseguindo, assim, uma vantagem indevida para si ou para outrem, com lesão patrimonial alheia. "

Compreenda que o crime de estelionato não se utiliza de furto ou de violência, quer seja física ou moral, o que realmente acontece é uma ilusão da vítima que coopera com o ato, mediante os meios fraudulento ou ardil.

Utilizando o mesmo raciocínio, é factível citar exemplos da conduta supracitada por meio digital, como a realização de empréstimos bancários com juros reduzidos, oferta de falsos empregos, que requer uma taxa para a inscrição ou até mesmo para conseguir o posto de trabalho, e o mais habitual de todos; a pirâmide financeira, que é o pagamento de um valor para entrar no sistema e, ao indicar um número determinado de novos membros, começa a receber dinheiro.

4.6 Invasão de dispositivo informático

A partir do momento em que surgem novas condutas no seio social, novos tipos penais prosperam nos ordenamentos jurídicos. Dessa forma, o conhecido brocardo latino "ex facto oritur ius" se agiganta na seara criminal.

Neste contexto que o crime de invasão de dispositivo informático foi inserido no Código Penal Brasileiro, por meio da Lei 12.737/2012, mais conhecida por "Lei Carolina Dieckman", uma vez que a renomada atriz teve extraídas de seu computador pessoal fotos íntimas e mensagens privadas, que foram compartilhadas na internet.

O tipo penal do crime de invasão de dispositivo informático está presente no art. 154-A, *in verbis*:

> 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:

Repara-se que o verbo invadir é o núcleo penal, já que tem como finalidade violar, acessar, indevidamente, aparelho que receba ou transmita dados. Ademais, é exigido que o dispositivo informático seja de outra pessoa e não de quem comete o delito.

No mesmo sentido, o bem jurídico tutelado está inserido tanto no capítulo que trata dos crimes contra a liberdade individual, do Código Penal brasileiro como no art. 5º, inciso X da Constituição Federal.

Assegurar a inviolabilidade da intimidade e da vida privada é cerne do artigo supracitado. Mendes e Coelho:

> O direito à privacidade, em sentido mais estrito, conduz à pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral. (MENDES e COELHO, 2007, p.370)

É indiscutível que a "Lei Carolina Dieckman", inovou em termos e expressões, dado que a falta de definição dos mesmos pode ocasionar dificuldades quanto à sai aplicação, tanto persecutória quanto processual. Adversidades como a pretensão punitiva, a disponibilidade do bem jurídico protegido, a tipificação do crime e a propagação de informações são problemáticas reiteradas no crime em questão.

5 CONCLUSÃO

Neste artigo procurou-se descrever e caracterizar os crimes cibernéticos, apontar os principais sujeitos e se pronunciar, de forma breve, sobre os crimes preponderantes que dele fazem parte.

Verificou-se, que os crimes virtuais podem ser desmembrados em puros ou próprios, que condutas perpetradas contra um sistema informático, sejam quais forem as motivações do agente e crimes virtuais abertos e impróprios, aqueles efetuados contra outros bens jurídicos, por meio de um sistema informático.

Os sujeitos do crime são divididos entre aqueles que cometem o ato ilícito e antijurídico, que tem a finalidade de ferir e violar o bem jurídico alheio por meio da internet e a pessoa que tem seu direito violado, ou seja, a vítima do respectivo ato. Como dito anteriormente, o causador do crime ou da infração, pode tanto ser um profissional e possuir um conhecimento elevado, e assim ser chamado de Hacker ou Cracker, quanto pode ser, também, um cidadão comum, sem qualquer tipo de conhecimento técnico, que fez uso da internet para cometer ato devidamente tipificado pelo nosso ordenamento jurídico.

Uma meditação sobre a classificação dos principais crimes virtuais para percepção de modo sistêmico de certos delitos já tipificados e os que ainda sofrem com lacunas e a sua falta de punição.

A sensação de impunidade para os autores dos crimes praticados por intermédio do computador, fará com que o encorajamento para que outros indivíduos pratiquem ações ilícitas semelhantes sejam maiores, pois impunidade proporciona mais impunidade. A adequada investigação e consequente punição dos autores são consideradas as principais inibidoras da sua incidência.

O direito digital é uma matéria contemporânea e por isso necessita de estudos aprofundados que intentem trazer maiores

referências e pesquisas sobre a relação do Direito Penal com o ambiente virtual.

Logo, é preciso que exista um trabalho conjunto, tanto por parte dos órgãos e instituições que atuam na persecução penal como daqueles que elaboram e modificam as legislações. A ação governamental precisa ser uniforme e se basear em intenções e desígnios harmônicos, dado que a sua ausência é visível, já que as ações integradas ainda são raras e baseiam-se de contatos pessoais e informais entre as partes que fazem parte do processo.

REFERÊNCIAS

BRASIL, Lei n. 2.848, de 07 de dezembro 1940. Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 17 mai. 2020.

BRASIL. Constituição (**1988**). Constituição da República Federativa do Brasil.

BRASIL. Lei 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: 24 mai. 2020.

CANALTECH. **O que são crackers e hackers? Qual a diferença entre eles e como combatê-los.** Disponível em: <https://canaltech.com.br/seguranca/o-que-e-cracker-hacker-diferenca/> Acesso em: 12 de mai. De 2020.

CANALTECH. **O que é um Lammer?** Disponível em: <https://canaltech.com.br/hacker/o-que-e-um-lammer/> Acesso em: 14 de mai. De 2020.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529>. Acesso em: 18 mai. 2020.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport Livros e Multimídia Ltda. 2014. E-book.

CONVENÇÃO SOBRE O CIBERCRIME. Budapeste, 23 nov. 2001. Disponível em: <https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185 Portugese.pdf>. Acesso em: 18 mai. 2020.

COSTA, Marco Aurélio Rodrigues. **Crimes de informática.** Disponível em: Revista Eletrônica Jus Navigandi<http://www.jus.com.br/doutrina/crinfo.html>. Acesso em: 18 mai. 2020.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** 1ª Ed. São Paulo: Saraiva, 2011. E-book.

DE ALMEIDA, Maria Paulo Castro. **A evolução no combate aos crimes virtuais**. Orientadores: Mônica Areal, Néli Luiza C. Fetzner, Nelson C. Tavares Junior, 2015. 17 f. Tese (Artigo Científico) - Escola da Magistratura do Estado do Rio de Janeiro. Rio de Janeiro. 2015.

FERREIRA, Ivette Senise. **Direito & Internet: Aspectos Jurídicos Relevantes**. 2 ed. São Paulo: QuartierLatin. 2005.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. Boletim do IBCCrim, São Paulo: IBCCrim, n. 95, ano 8, out. 2000.

GRECO, Rogério. **Curso de Direito Penal: parte especial** - v. III. 7ª ed. Niterói: Impetus, 2009.

GRECO, Rogério. **Código Penal: comentado**. 10ª ed. – Niterói, RJ: Impetus, 2016.

IIMA. Instituto Information Management. **O cibercriminoso pode ser você!** Disponível em: <https://docmanagement.com.br/07/13/2018/o-cibercriminoso-pode-ser-voce/> Acesso em: 18 mai. 2020.

KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da criminalidade no cyberespaço** / de Santana : Universidade Estadual de Feira de Santana, 2017. E-book.

LOPES, Alan Moreira. **Crimes praticados por meio eletrônico**. 1ª Ed. Curitiba: Ag Book, 2012.

MENDES, G. F.; COELHO, I. M.; BRANCO, P. G. G. **Curso de direito constitucional**. São Paulo: Saraiva, 2007.

MIRABETE, Julio Fabbrini. **Manual do Direito Penal: parte geral.** 24 ed. São Paulo: Atlas, 2008.

MIRABETE, Julio Fabbrini. **Manual de direito penal, vol. 2: parte especial.** 25. Ed. São Paulo: Atlas, 2008.

NUCCI, Guilherme de Souza. **Manual de direito penal: parte geral: parte especial**. 6ª Ed., São Paulo: RT, 2009.

OLIVEIRA, Wilson José. **Dossiê hacker: técnicas profissionais para conhecer e proteger-se de ataques**. São Paulo: Digerati Books, 2006.

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

PRADO, Luiz Regis. **Curso de direito penal Brasileiro: volume II, parte especial**. 15 ed. São Paulo. RT. 2008.

ROQUE, Sérgio Marcos. **Criminalidade Informática – Crimes e Criminosos do Computador**. São Paulo: ADPESP Cultural, 2007.

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

ROSSINI, A. E. S. et al. (2004). **Informática, telemática e direito penal.** São Paulo: Memória Jurídica.

TANAKA, Caroline Yumi de Oliveira. OS CRIMES CONTRA A HONRA E A INTERNET. 2016. Disponível em: <http://repositorio.uniceub.br/bitstream/235/9234/1/21204599.pdf>. Acesso em: 18 mai. 2020.

UNYLEYA. **Afinal, qual é a diferença entre hacker e cracker?** Disponível em: <https://blog.unyleya.edu.br/bitbyte/diferenca-entre-hacker-e-cracker/> Acesso em: 18 mai. 2020.

VIANA, Marco Túlio apud CARNEIRO, Adeneele Garcia. **Fundamentos de direito penal informático. Do acesso não**

autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.

ZAFFARONI, Eugenio, PIERANGELI, José. **Manual de Direito Penal – parte geral**. Ed 4°, Tribunais, 2001.

AS FORMAS DE FRAUDES ECONÔMICAS NA ERA DIGITAL

Eduardo Andrade Pacheco Amoras[1]

RESUMO

O presente artigo tem por objetivo analisar e compreender os meios fraudulentos que criminosos procuram obter vantagem ilícita por meio da internet. Terá como proposta analisar estes crimes virtuais e as suas consequências jurídicas quanto aos atos ilegalmente praticados. Serão abordados diversos dispositivos legais que refletem diretamente nos crimes praticados a fim de obter vantagem econômica em face das vítimas.

Palavras-chave: Fraude. Ocultação de bens. *Phishing*. Pirâmide Financeira. Crimes contra a economia popular.

ABSTRACT

This article aims to analyze and understand the fraudulent means that criminals seeks to gain illicit advantage through the internet. It will analyze these virtual crimes and their legal consequences regarding those acts illegally practiced.

Keywords: Fraud. Concealment of goods. Phishing. Financial pyramid. Crimes against the popular economy.

[1] Advogado formado pelo Centro Universitário de Brasília – UniCEUB. Aluno do curso de pós-graduação lato sensu do Centro Universitário de Brasília – UniCEUB/ICPD.

1 INTRODUÇÃO

É sabido que o mundo é uma constante variável que muda ao decorrer do tempo. É certo que desde os primórdios da humanidade até os dias de hoje houve uma enorme evolução cientifica nas mais diversas áreas, seja ela na medicina, na tecnologia, na matemática, e até mesmo no Direito. É possível concluir que o mundo está, e sempre estará avançando e adaptando-se rumo às inovações tecnológicas.

Destaca a assertiva acima para aproximar o avanço mundial na tecnologia para o bem. Contudo, sabemos que se pode ser usado para causar prejuízo a outrem.

A esfera criminal não é bastante longe da realidade do avanço tecnológico. Os crimes cometidos estão também se adaptando ao mundo da tecnologia. Com o advento da internet e computadores, criminosos buscam cada vez mais alternativas para cometer seus delitos no meio virtual acreditando ser um espaço onde a lei não possa alcança-los.

Existem diversos crimes cometidos na internet passíveis de aplicação da lei, seja ela em esfera cível, penal ou administrativa. O fato é que dentre estes crimes, os mais comuns são os crimes contra a honra publicados em redes sociais, crimes de ódio, crimes de divulgação de imagens não autorizadas, e crimes que buscam vantagens econômicas.

Neste contexto, ressaltam-se os criminosos que buscam obter vantagem de origem ilícita preferem cometer o crime de estelionato. Estes indivíduos usam de sua inteligência para enganar e subtrair bens de pessoas de boa-fé. O estelionato é um crime comum e que já existia antes mesmo do surgimento e ascensão da internet.

2 BREVE CONCEITO E CONSIDERAÇÕES ACERCA DO CRIME DE ESTELIONATO

Tratando-se de crime fraudulento, o estelionato está previsto no artigo 171 do Código Penal Brasileiro, trazendo consigo a definição de 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.

No crime de estelionato previsto no artigo 171 do Código Penal, é importante frisar que no crime de estelionato, há o empenho do criminoso para com que a vítima entregue a coisa voluntariamente, sem saber que está sendo enganada.

A título de exemplo, o estelionato era e ainda é praticado na compra e vendas de celulares particulares. É o caso do individuo de boa-fé que anuncia algum tipo de eletrônico particular podendo ser um celular, câmera fotográfica ou até mesmo um computador. O criminoso, desta forma, entra em contato com a vítima com intuito de efetuar a compra. Usando de uma historia fantasiosa, o criminoso convence a vítima a entregar voluntariamente o produto à venda, sob a promessa de que o pagamento já foi feito mediante deposito no caixa eletrônico. Contudo, esta versão não prospera pois o criminoso jamais fez o deposito no caixa eletrônico, enganando a vítima e fazendo acreditar na conclusão do negócio.

Nota-se que este é um dos métodos de estelionato mais comuns existentes e praticados, não só antigamente como também nos dias atuais.

Por outro lado, por ser um crime tão comum, e que não deixa de ser menos ilícito, já não surte tanto efeito nas vítimas como antigamente. O crime, infelizmente, acompanha o progresso e avanço tecnológico do mundo. Por isso, criminosos experientes na

área decorrentes de anos de pratica vêm inovando cada vez mais, partindo para a prática destes e outros crimes no meio digital.

2.1 As Fraudes No Meio Digital

Desesperados para "manter-se no mercado", criminosos buscam cada vez mais inovar suas técnicas para enganar indivíduos de boa-fé e obter vantagens ilícitas em desfavor dos mesmos, causando muita das vezes, enorme prejuízo financeiro. Neste sentido, é importante a reserva deste presente capítulo para descrever e exemplificar como estes indivíduos vêm cometendo estes tipos de crimes no meio digital atualmente, visto que a proposta do presente artigo é disseminar informação e dificultar ainda mais a prática e obtenção das vantagens ilícitas por estes criminosos.

2.1.1 "O Golpe Do Empréstimo Fácil"

A primeira delas é o golpe do empréstimo fácil. Consiste no envio de SMS, e-mail, ou até mesmo em ligações onde o estelionatário sabendo da difícil condição financeira da vitima, se aproveita para ofertar empréstimos com juro bastante abaixo do praticado no mercado financeiro. Atraída pela proposta, o criminoso condiciona o empréstimo do valor solicitado pela vitima a um depósito bancário, de valor menor, como caução. Geralmente a vítima acaba por depositando o valor na conta do estelionatário, e consequentemente jamais irá reaver o dinheiro depositado a título de caução, como evidentemente, jamais receberá o valor do empréstimo.

Para evitar ser vítima desse tipo de golpe, recomenda-se sempre desconfiar de indivíduos que condicionam o empréstimo

mediante deposito bancário prévio, assim como sempre procurar instituição financeira com experiência no mercado financeiro[2].

2.1.2 "Golpes Em Sites De Venda"

Este é um exemplo mais complexo e por isso, bastante utilizado no meio criminoso. É o caso de anúncios de venda de objetos na internet como OLX e Mercado Livre. A vítima, que no caso é a pessoa que anuncia seu produto em determinado site de venda, obtém rapidamente uma resposta do estelionatário, que neste caso, se passa como suposto comprador. O estelionatário envia diversas mensagens afirmando interesse no produto, contudo, alega não morar no estado da vítima, requerendo que o produto seja despachado via Correios até ele. Negociado o valor entre a vítima e o estelionatário, o estelionatário geralmente efetua o suposto pagamento mediante depósito e envia uma foto do comprovante para a vítima. Prontamente, a vítima de boa-fé acredita no pagamento e acaba enviando imediatamente o produto anunciado. Ocorre que o valor depositado jamais irá entrar na conta da vítima, uma vez que os criminosos costumam depositar envelopes vazios no caixa eletrônico, ou até mesmo falsificando o comprovante de depósito.

Acontece também caso em que a vítima opta pela plataforma do Mercado Livre por ser supostamente mais segura, por ter uma função denominada em inglês como *escrow*, ou em tradução livre, garantia. Essa função visa garantir mais segurança tanto para quem compra como para quem vende. Consiste no depósito do valor da mercadoria na conta da plataforma, no caso Mercado Livre, e este valor somente é liberado para a conta bancaria do

[2] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** São Paulo: Brasport 2014, p. 124.

vendedor quando o produto chega às mãos do comprador. Assim, o comprador tem a segurança de que se o produto não chegar em seu destino final, terá seu dinheiro ressarcido, uma vez que o valor estará em posse da plataforma de venda.

Contudo, estelionatários usam dessa função para desfavorecer o vendedor, no caso vítima. A situação é a mesma acima descrita, com um único diferencial. Ocorre que o criminoso cria um nome de e-mail falso se passando pela plataforma, no caso Mercado Livre, e enviam para a vítima uma mensagem fraudulenta e fidedigna ao original alertando que o produto pode ser enviado visto que o pagamento foi aprovado. A vítima depositando sua confiança na plataforma e no corpo do e-mail idêntico ao original envia o produto ao criminoso. Consequentemente, a vítima jamais irá receber o valor do produto, e por outro lado, o estelionatário irá receber o bem.

Para evitar este tipo de estelionato, sempre verifique o domínio do e-mail recebido. Um e-mail é composto por um nome seguido de um domínio onde é hospedado o e-mail. O domínio é sempre o que vem depois do símbolo "@". Geralmente plataformas como o Mercado Livre detém domínio próprio, isto é, possui e-mail cujo final é "@mercadolivre.com.br". Se ocorrer de receber um e-mail e não tiver o domínio da plataforma, certamente é uma tentativa de estelionato.

Em todos os casos, é fortemente recomendado que sempre comunique a autoridade policial acerca da tentativa ou até mesmo da consumação do crime de estelionato, uma vez que se abre uma investigação para apurar o fato criminoso[3].

[3] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** São Paulo: Brasport 2014, p. 138-139.

2.1.3 "Phishing – Páginas De Internet Falsas"

A palavra *phishing* tem origem inglesa e é derivada da palavra *fishing*. Este tipo de dialeto vem a ser comumente utilizado na obtenção ilícita de dados pessoais de indivíduos que acessam a sites fraudulentos acreditando ser legítimos.

Em outras palavras, trata-se de sites criminosos e fraudulentos que tem sua arquitetura e aparência idêntica a de um site legitimo e original com a finalidade de "pescar" dados. Neste caso, criminosos enviam links de sites para as vitimas, e as mesmas acabam por acessando o site acreditando ser o original e informando dados pessoais indevidamente.

É comum que criminosos "montem" uma página falsa de internet idêntica a de bancos ou instituições financeiras, como do Banco do Brasil, Caixa Econômica, dentre outras. Assim, enviam o link do site fraudulento por meio de SMS, e-mails, ou outro aplicativo de mensagem, para várias potenciais vítimas. Aquela vitima que porventura acessa o site fraudulento e seus dados pessoais, acabam por enviando os dados para o criminoso, ou grupo criminoso, que agora tem posse destas informações sensíveis.

Neste sentido, e em posse destes dados, os criminosos podem usar estas informações para praticar diversos outros delitos, dentre eles, subtrair o valor da conta bancária da vítima.

Um estudo realizado por uma empresa especializada em cibersegurança PSafe, mostra um aumento nos ataques cibernéticos. Dentre eles, a pesquisa mostra que no último trimestre do ano de 2018, foram registrado cerca de 63,8 milhões de links maliciosos, sendo que deste 63,8 milhões de links

maliciosos, cerca de 57,4% eram links phishing por aplicativos de mensagem, e 3,8% de links de phishing bancários[4]. (citar referencia)

A título de exemplo, pode ocorrer de um criminoso, ou um grupo dos mesmos, criarem um site de vendas e anunciar produtos com valores bem abaixo daqueles praticados normalmente pelo mercado. Atraída pelo valor anunciado nos produtos anunciados, a vítima costuma efetuar o pagamento. Em situações como acima descrita, é recomendado que o indivíduo ao encontrar com sites com preços chamativos, consulte a reputação do site de venda em outros sites confiáveis, tais como www.reclameaqui.com.br e www.confiometro.com.br.

Esta técnica de fraude merece melhor atenção, e por isto, será mais bem debatido posteriormente.

2.1.4 "As Pirâmides Financeiras"

A pirâmide financeira é caracterizada pela criação de uma suposta instituição financeira, por um ou mais criminosos, em que se procuram indivíduos de boa-fé para investir e adentrar a falsa sociedade. Uma pirâmide financeira geralmente buscam vítimas para integrar e investir a organização sob a promessa de alta rentabilidade por mês, prometendo, por vezes, que o valor investido seja duplicado ou até triplicado em um lapso temporal pequeno.

[4] PSAFE, dfndrlab. Relatório da Segurança Digital no Brasil Segundo trimestre - 2018. Disponível em: https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf. Acesso em: 01 de junho de 2020.

Assim, a vítima tentada pelo alto valor lucrativo prometido pela suposta instituição financeira, investe seu dinheiro e adentra a organização de forma legitima. Contudo, a vítima ao adentrar e investir seu dinheiro na falsa instituição financeira tem o seu lucro devido condicionado ao ingresso de outros indivíduos. Desta forma, a vítima somente receberia o suposto lucro investido na falsa instituição se o mesmo convidasse duas ou mais pessoas para integrar e investir na instituição.

Para promover a instituição fraudulenta, os criminosos usam deste valor investido por outros de boa-fé para ocultar a origem ilícita deste dinheiro, fazendo-a ter uma aparência lícita. Efetuam diversas compras como carros de luxo, imóveis de alto poder aquisitivo, e em outros negócios, e exibem em redes sociais para dar a falsa aparência de que seu negócio fraudulento prospera.

É intuitivo que, mediante a promessa de alta rentabilidade e o condicionamento de ingresso de outras pessoas como investidores, haverá um crescimento exponencial de indivíduos investindo em uma instituição fraudulenta.

Ocorre que quando o esquema criminoso obtém altos níveis investimentos, os criminosos desaparecem com o valor investido daqueles que ingressaram na instituição financeira acreditando ser um negócio licito e legítimo. Usam diversos meios para ocultar os valores investidos. Usam dados pessoais de outras pessoas, que podem ou não fazer parte da organização criminosa, para fazer transações financeiras e movimentar os valores até que se tornem difíceis de serem recuperados.

É o caso da KriptaCoin, instituição financeira fraudulenta em que os sócios prometiam alta rentabilidade para quem investisse na operação. Tratava-se de um esquema fraudulento em que os

sócios ofertavam um tipo de moeda virtual atraindo as vítimas com rendimento de 1% ao dia. Nesta operação, as vitimas que investiam seu dinheiro somente poderiam resgatar o lucro depois de um ano. Ademais, os criminosos incentivavam as vítimas a convidarem outras vitimas, prometendo um bônus de 10% para cada pessoa que adentrasse o esquema fraudulento. Não é necessário afirmar que tempos após, as vitimas não tiveram êxito em resgatar o valor investido[5].

Neste sentido, é extremamente aconselhável que jamais confie em instituições que prometem lucros exorbitantes. E se tiver sido vítima deste tipo de fraude, sempre procure e comunique a autoridade policial.

3 OS ASPECTOS JURÍDICOS DOS CRIMES DIGITAIS

Amplamente debatidos acerca de algum dos crimes mais comuns praticados em meio digital em que se objetiva a vantagem econômica, é necessário debater acerca dos aspectos e consequências jurídicas que estes crimes trazem consigo.

A fraude do falso empréstimo, assim como a fraude nos sites de venda, é a forma mais simples do crime de estelionato contido no artigo 171 do Código Penal Brasileiro. Trata-se de um individuo que envia mensagens, seja qual for o meio, com a finalidade de atrair vitimas desesperadas por um meio de empréstimo fácil e desburocratizado. Como debatido no tópico acima, a vítima é condicionada a efetuar um deposito caução na conta do criminoso, sob pena de não obter o suposto crédito aceito.

[5] PULJIZ, Mara. Moeda virtual falsa foi usada por quadrilha em 'pirâmide financeira' no DF e em Goiás. Disponível em: https://g1.globo.com/distrito-federal/noticia/policia-civil-do-df-desarticula-esquema-de-piramide-financeira-que-movimentou-r-250-milhoes.ghtml. Acesso em: 01 de junho de 2020.

Ocorre que a conta em que se é depositada o valor caução muita das vezes não é do criminoso que solicita. Nem mesmo de alguém que participa do grupo criminoso. Trata-se de contas cujas informações da titularidade são falsas. Em outras palavras, os estelionatários abrem contas bancárias usando dados pessoais falsos, obtidos ilegalmente, incorrendo em diversos outros crimes também tipificados na lei penal. Não obstante o crime de estelionato previsto no artigo 171, para obter a vantagem ilícita, utilizam dados pessoais falsos para abrir contas bancárias, incorrendo no crime de falsidade ideológica previsto no artigo 299 do Código Penal Brasileiro. Acredita-se que na maioria das vezes, trata-se de um grupo organizado e voltado para este tipo de crime, incorre no crime previsto no artigo 288 do referido diploma legal.

Em se tratando de sites falsos que detenha aparência verdadeira, denominadas como sites *phishing*, tem uma definição jurídica diferente do estelionato, previsto no artigo 171 do Código Penal. Estes sites tem o único intuito de levar a erro a vítima, fazendo com que ela insira dados pessoais e envie para o agente mal intencionado.

Neste sentido, estes sites têm como objetivo simular uma verdadeira empresa ou instituição. Diversos são os modos que estes agentes utilizam, desde sites parecidos com instituições financeiras, vendas de produtos, ou organizações diversas. Utilizam de vários métodos de disseminar os links desses sites, sendo eles por SMS, e-mails, ou qualquer outra rede social.

Ao acessar sites fraudulentos que dão a crer que são de uma instituição válida, as vítimas informam dados pessoais indevidamente. Na hipótese do acesso em sites de vendas fraudulentas, as vítimas efetuam compras os quais são debitados de sua conta bancária, porém o produto adquirido jamais será

entregue. De igual modo será se a vítima acessar um site fraudulento acreditando ser de seu banco. A vítima ao inserir seus dados bancários, envia esta informação para outro destino.

Ocorre que inserir estes tipos de informações pessoas em sites fraudulentos acarreta em diversas consequências negativas para a vítima. Em posse de dados pessoais, os criminosos podem usar desses dados para subtrair valores das contas bancárias das vítimas, assim como utilizar dessas informações pessoais para abrir contas em bancos, abrirem empresas, dentre outros.

Embora deixe transparecer que se trata de um estelionato comum, esta não é uma afirmativa correta. Isto porque o crime de estelionato tem como elemento caracterizador a entrega voluntária do objeto. O criminoso sabe quem é a sua vítima, como é o caso das fraudes em sites como OLX e Mercado Livre, onde a vítima e o estelionatário mantém diálogo a fim de obter o consentimento da vítima em entregar a coisa.

Não é o que efetivamente ocorre em sites fraudulentos bancários, ou sites *bank-phishing*. Sites como estes induzem a vítima a entregar dados bancários pessoais sem saber que está sendo iludida por uma imitação do site original. Neste sentido, ensina Fernando Capez que a fraude que qualifica o furto é meio ardil empregado pelo agente para diminuir a vigilância da vítima sobre a coisa e realizar a subtração, ao passo que, no estelionato, é a própria vítima que, iludida, entrega voluntariamente o bem ao agente[6].

Neste caso, havendo a entrega de dados pela vítima e caso venha a ter algum valor subtraído de sua conta bancária, o agente

[6] CAPEZ, Fernando. **Curso de direito penal: parte especial**. v. 2. 10. ed. de acordo com as Leis n. 12.015 e 12.033 de 2009. 2. tir. São Paulo: Saraiva, 2010, p. 449.

passivo do furto qualificado por meio fraudulento, nos termos do artigo 155 paragrafo 4º do CP, é a própria instituição financeira, isto porquê a instituição financeira possui a guarda do valor, conforme se extrai do voto da *Ministra Maria Thereza de Assis Moura, do STJ, em Conflito de Competência* nº 72.738/RS. *In Verbis:*

> "O cerne da questão para se determinar o Juízo competente para o prosseguimento do caso em tela reside, pontualmente, na correta capitulação da conduta criminosa em comento.
>
> O furto mediante fraude, escalada ou destreza não se confunde com o estelionato. No primeiro, a fraude visa a diminuir a vigilância da vítima, sem que esta perceba que está sendo desapossada; há discordância expressa ou presumida do titular do direito patrimonial em relação à conduta do agente. No segundo, a fraude visa a fazer com que a vítima incida em erro e, espontaneamente, entregue o bem ao agente; o consentimento da vítima integra a própria figura delituosa.
>
> Da análise dos autos, verifica-se que trata de hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de três mil e quatrocentos reais de conta bancária situada em Porto Alegre/RS, por meio da Internet Banking da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima.
>
> A fraude, de fato, foi usada para burlar o sistema de proteção e vigilância do Banco sobre os valores mantidos sob sua guarda, configurando, assim, crime de furto qualificado por fraude, e não estelionato (STJ, CC nº 72.738, RS 0226850-1/2006, Rel. Ministra Maria Thereza de Assis Moura, j. 08/08/2007, Dj 20/08/2007)."

Por outro lado, existem outros sites *phishing* que também têm o objetivo de pesca de dados pessoais, não necessariamente para invadir a conta bancária da vítima, mas pode causar prejuízo econômico. Estes são geralmente sites de venda de produtos, atraindo as vítimas por anúncios de preços baixos das

mercadorias. Efetuado a compra no falso site de vendas de produtos, os criminosos usam destas informações para subtrair valores da conta da vítima. Perceba que o simples fato de informar os dados do cartão de crédito ou efetuar pagamento mediante boleto não se caracteriza a invasão da conta bancária da vítima.

Neste sentido, donos de sites como estes incorrem nos crime de possível formação de grupo no intuito de cometer crime previsto artigo 288 do Código Penal, falsidade ideológica previsto no artigo 299 do Código Penal, e crimes previstos na lei 9.613/98 (que trata da "lavagem" de dinheiro e ocultação de bens), como também contra a economia popular disciplinado na lei 1521/51, em que se trata em seu artigo 2º, IX acerca da obtenção ou a tentativa de obter ganhos ilícitos em detrimento do povo ou de número indeterminado de pessoas mediante especulações ou processos fraudulentos.

Já as pirâmides financeiras operam de modo diferente, mas não menos fraudulento. Tem como objetivo captar investidores sob a promessa de alta rentabilidade após um curto período de tempo. Diversas são as condições para o resgate e características de uma pirâmide financeira. A principal característica de uma pirâmide financeira se encontra no incentivo da instituição fraudulenta em convidar novos indivíduos a integrar a plataforma de investimento, e altíssima rentabilidade no mercado financeiro.

Os criminosos usam do alto valor arrecadado por investidores para efetuar compras de veículos de luxo, imóveis de luxo, dentre outros meios de investimento, com a finalidade de propagar para o público acerca do sucesso dos investimentos. Ocorre que muita das vezes estes falsos empresários sócios de instituições financeiras comumente conhecidas como pirâmides financeiras, acabam por nunca retornar o valor investido acrescidos do lucro

aos verdadeiros investidores. Lesam então diversos indivíduos de boa-fé que adentram a sociedade atraída pela alta rentabilidade.

Este tipo de crime pode ser enquadrado em diversos dispositivos legais. Pelo fato de criarem uma falsa instituição financeira que promete rentabilidade acima dos quais são praticados no mercado financeiro, cometem o crime contra a economia popular disciplinado na lei 1.521/51, em que se trata em seu artigo 2º, IX. Os valores investidos por indivíduos de boa-fé são transformados em ativos lícitos, onde efetuam compras de carros e imóveis de luxo, caracterizando o crime de ocultação de bens, previstos na lei 9.613/98. Ademais, cometem diversos outros crimes como a de formação de grupos para cometer crimes, falsidade ideológica, ameaça a eventuais investidores que queiram resgatar seus ativos, dentre outros.

Tais leis penais que tipificam estes tipos de condutas se mostram extremamente ultrapassadas pelo decorrer do tempo, sendo certo que a lei deve sempre acompanhar a evolução de uma sociedade.

Ante todo o exposto neste capítulo, mostra-se necessário a atualização da lei penal brasileira para acompanhar o ritmo crescente da evolução informática como também as artimanhas praticadas pelos criminosos, uma vez que tais legislações mostram-se obscuras e sem grandes efeitos a fim de inibir praticas criminosas por meio da internet ou outro meio digital.

4 CONCLUSÃO

O presente artigo teve como objetivo analisar os crimes de fraudes, tais como estelionato, furto, dentre outros. Ateve-se especificamente aos métodos utilizados por criminosos em meios

digitais para obter vantagem financeira, como pirâmides financeiras, sites *phishing*, e outros meios de estelionato. Em primeiro momento foi analisado os métodos utilizados pelos criminosos na pratica de obter ilicitamente as vantagens econômicas procurando exemplificar e dar dicas para que estas artimanhas caiam em desuso. Foram analisados casos concretos, tais como o da KriptaCoin, em que sócios da empresa engaram os investidores sob o falso argumento de uma moeda digital em ascensão traria altos lucros.

Posteriormente foram analisadas as consequências jurídicas deste tipo de pratica em que se procura obter vantagens econômicas ilicitamente. Conclui-se que as praticas destes crimes virtuais não têm uma legislação especifica, além da lei 12.965/2014. Práticas como *phishing* e pirâmides financeiras no meio digital ainda refletem as leis ultrapassadas, onde por vezes, acabam por ser obscuras para punir aqueles que tanto praticam estes crimes que lesam o patrimônio das vitimas.

REFERÊNCIAS

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília: Senado, 1988.

_____. Código de Processo Penal. decreto lei nº 3.689, de 03 de outubro de 1941. Disponível em: http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del3689.htm

_____. **Lei Nº 1.521, De 26 De Dezembro De 1951..** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l1521.htm

_____. Código Penal. Decreto lei nº 2.848, de 07 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

_____. Lei Nº 9.613, De 3 De Março De 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

BERGO, Thaís Rosenbaum e HARO, Guilherme Prado Bohac de (2014). **Conceituação De Pirâmide Financeira E Suas Diferenças Em Relação A Marketing Multinível**. Revista Encontro de Iniciação Científica. Disponivel em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/download/4402/4162.

CAPEZ, Fernando**. Curso de direito penal: parte especial**. v. 2. 10. ed. de acordo com as Leis n. 12.015 e 12.033 de 2009. 2. tir. São Paulo: Saraiva, 2010.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** São Paulo: Brasport 2014.

DOMINGOS, Fernanda Teixeira Souza e RÖDER, Priscila Costa Schreiner. **Obtenção De Provas Digitais E Jurisdição Na Internet.** Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes

FILHO, Democrito Reinaldo**. A Infecção Do Sistema Dns: a nova modalidade de *phishing* e a responsabilidade do provedor**. Disponível em: https://www.imn.org.br/artigos/ver/23

FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos.** Disponível em: https://jus.com.br/artigos/77225

GOMES, Rebeca Bravo de Oliveira e SILVA, Marcelo Sarsur Lucas da. O ENQUADRAMENTO JURÍDICO PENAL DO PHISHING E SUAS REPERCUSSÕES NO FURTO INFORMÁTICO. Disponível em: http://revistas.newtonpaiva.br/letras-juridicas/?p=964

PINHEIRO, Thaís Rodrigues. **FURTO MEDIANTE FRAUDE X ESTELIONATO ASPECTOS PENAIS E REPERCUSSÃO DA FRAUDE CIVIL NO ÂMBITO CRIMINAL.**Disponível em: https://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/2semestre2011/trabalhos_22011/ThaisRPinheiro.pdf

PSAFE, dfndrlab. **Relatório da Segurança Digital no Brasil Segundo trimestre - 2018.** Disponível em: https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-

Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf. Acesso em: 01 de junho de 2020.

PULJIZ, Mara. **Moeda virtual falsa foi usada por quadrilha em 'pirâmide financeira' no DF e em Goiás.** Disponível em: https://g1.globo.com/distrito-federal/noticia/policia-civil-do-df-desarticula-esquema-de-piramide-financeira-que-movimentou-r-250-milhoes.ghtml. Acesso em: 01 de junho de 2020.

SILVA Beronalda Messias da, e ASSIS, Mariana Redondo de. **PHISHING DE INTERNET, COMO CRIMINALIZAR? ASPECTOS TÉCNICOSE JURÍDICOS DESSA AMEAÇA VIRTUAL.** Disponível em: http://www.publicadireito.com.br/artigos/?cod=6840f4a1c1d16484

TEIXEIRA, Filipe Silva e CHAVES, Fábio Barbosa. **Os crimes de fraude e estelionato cibernéticos e a proteção ao consumidor no e-commerce.** Disponível em: https://jus.com.br/artigos/73480/os-crimes-de-fraude-e-estelionato-ciberneticos-e-a-protecao-ao-consumidor-no-e-commerce

WENDT, Emerson e JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: Ameaças e Procedimento de Investigação.** 2ª. Ed. São Paulo: Brasport 2013.

A NECESSIDADE DE ELEVAÇÃO DA PROTEÇÃO DE DADOS AO STATUS DE DIREITO FUNDAMENTAL

Ana Luíza Gomide do Nascimento[1]

RESUMO

O presente trabalho visa demostrar a necessidade da elevação da proteção aos dados pessoais à um direito fundamental constitucionalmente protegido. No primeiro capítulo há uma conceituação e explicação do que são dados pessoais, bancos de dados e tratamento de dados. No segundo capítulo há uma breve explicação dos princípios expressos no art. 6º da LGPD e da sua importância. No último capítulo buscou-se demonstrar a necessidade da proteção de dados em ser considera um direito fundamental e de exemplificar que já há princípios próprios e que a sociedade carece de tal proteção, explicou-se que não pode ser considerado apenas uma extensão do direito de privacidade ou da personalidade, mas que, de fato, é mais um direito no rol do direito de personalidade de cada indivíduo.

Palavras-chave: LGPD. Direito Fundamental. Proteção de Dados.

ABSTRACT

The present work aims to demonstrate the necessity of the elevation of protection of personal data to a fundamental right that is constitutionally protected. At the first chapter there is a concepltualization and explanation about what is data people, database and data processing. At the second chapter there is a brief explanation about the expressed principles on Article 4 of LGPD and its importance. On the last chapter sought to demonstrate the necessity of protection of data being considered a fundamental right and to exemplify that there is already its own

[1] Advogada. Aluna do curso de pós-graduação *lato sensu* do Centro Universitário de Brasília – UNICEUB/ICPD.

principles and that the society needs this protection, explained that can't be considered only a extension of the privacy or the personality rights, but that indeed is one more right at the list of the personality right of each person.

Keywords: LGPD. Fundamental Rights. Data Protection.

1 INTRODUÇÃO

O presente estudo tem como objetivo demonstrar a necessidade da elevação da proteção de dados a um direito fundamental constitucionalmente protegido afastando a possibilidade de ser apenas parte integrante do direito à privacidade e de ser apenas uma extensão dos direitos de personalidade.

Essa diferenciação se mostra importante frente as inovações tecnológicas que trazem à baila novos problemas tais como os que o tratamento automatizado de dados pode causar. Os dados de um determinado titular dizem muito mais sobre ele que o próprio CPF ou RG pois tem a capacidade de demonstrar tudo sobre o indivíduo.

Os dados pessoais não são apenas características físicas, são características da personalidade da pessoa, sendo que o detentor dessas informações possui um verdadeiro dossiê do titular, podendo lhe oferecer exatamente e apenas produtos que gosta, além de poder vender exatamente da forma que a pessoa prefere comprar.

Esses são denominado dados sensíveis pois ensejam a possibilidade de causar discriminação ao realizar o tratamento desses. São sensíveis pois caracterizam a personalidade da pessoa, expressando exatamente a posição política, religião e opinião sobre assuntos diversos.

A falta de uma proteção constitucional e o não reconhecimento desde direito como um direito fundamental coloca em risco toda a sociedade pois a proteção é diretamente o resguardo dos cidadãos que a compõe. É possível ter noção, ao saber o quanto esses dados dizem sobre nós, a clara necessidade de uma proteção e uma rigorosa fiscalização, além de eventual multa.

Observada essa necessidade é necessário entender que é um direito autônomo pela sua importância, não podendo ser apenas uma extensão de outros para que seja garantida uma proteção total.

Outro ponto que merece destaque é a possibilidade da autodeterminação informacional por meio do consentimento, esse que é uma das bases legais que permitem a coleta e o tratamento de dados conforme a LGPD autoriza, e é a chave para que seja amplamente garantida a proteção constitucional assim como as outras bases legais que serão exemplificadas.

2 DADOS PESSOAIS, BANCO DE DADOS E TRATAMENTO DE DADOS

Antes de iniciar ao tema proposto, válido é conceituar o núcleo do mesmo. Afinal, o que são dados pessoais e como eles podem identificar uma pessoa a tal ponto de ser necessário que evolua a sua proteção ao status de direito fundamental.

2.1 Dados Pessoais

O dado pessoal é, de fato, o conceito mais importante a ser compreendido, pois todos os outros então ao seu redor. O conceito trazido por Patrícia Pinheiro é

Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva.[2]

Assim, os dados pessoais são todos e quaisquer tipos de informações que advém do seu titular. Que podem, por sua vez, serem especificados como dados sensíveis, que são aqueles que caracterizam a personalidade de seu titular, expressando a sua posição política, religião, orientação sexual, etc.

Outra espécie de dados pessoais são os dados anônimos, definido no art. 5º, inciso XI da LGPD que são dados que, por mais que seja referente a uma pessoa, ele não é capaz de identifica-la.

Para ser definido como dado anônimo, ele precisou passar por um processo de anonimização que se for refeito não poderá chegar ao seu titular, caso seja possível reverter esse processo, não será considerado um dado anônimo.[3]

2.2 Banco de Dados e Tratamento dos Dados Pessoais

Além da conceituação dos dados pessoais, necessário é conceituar o local onde é armazenado e explicitar a forma como é

[2] PINHEIRO, Patrícia. Conceitos e terminologias. In: PINHEIRO, P. P. **Proteção de dados pessoais - comentários à Lei n. 13.709/2018 LGPD.** São Paulo: Saraiva Educação, 2018. p. 25.

[3] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

tratado. Os dados são armazenados em um banco de dados, que é a estruturação dessas informações em um meio eletrônico ou não.[4]

Nota-se que não são apenas um apanhando de dados aleatórios, mas sim dados capazes de identificar o seu titular, armazenados de uma forma estruturada para que a pessoa que o for manipular, possa analisar e tomar decisões.[5]

A Lei Geral de Proteção de Dados (LGPD) além de conceituar todos esses termos e diversos outros que são importantes de igual forma, busca não apenas definir a proteção ao ato de deter esses dados mas, principalmente ao tratamento dos mesmos.

O tratamento de dados é definido por toda operação realizada com os dados pessoais, desde a coleta passando pela produção, recepção, classificação, utilização, acesso, armazenamento até a exclusão total desses.[6]

O tratamento dos dados pessoais devem seguir à risca a legislação específica pois será basicamente o compartilhamento de informações específicas dos seus titulares. O art. 6º e o 7º da LGPD define os princípios e as hipóteses em que esse tratamento de dados deverá se pautar.

A LGPD é uma legislação em sua essência principiológica, porém com todos esses princípios expressos, a fim de explicar e implementar na sociedade todos os assuntos abordados. Os

---

[4] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

[5] BIONI, Bruno. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.p. 32.

[6] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

princípios são verdadeiros norteadores da forma de aplicação da lei.

Além de conceituar esses termos, a LGPD também deu nome a quem lida com esses dados. O art. 5º[7], terminantemente conceitual, define o nome para o dono dos dados, para quem irá trata-los e outros mais:

> Art. 5º Para os fins desta Lei, considera-se:
>
> [...]
>
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
>
> IX - agentes de tratamento: o controlador e o operador;

Essas nomenclaturas são importantes para compreender exatamente quem é o responsável por cada etapa da proteção de dados, desde a sua coleta à tomada de decisões de como descartar os dados.

A lei define exatamente cada sujeito nessa relação para poder responsabiliza-lo por suas ações. Tal como na relação de consumo se faz necessário a conceituação de quem é consumidor e

[7] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

quem é fornecedor, de igual forma é preciso definir na proteção de dados.

3 OS PRINCÍPIOS UTILIZADOS NA PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados, em seu art. 6º[8], definiu dez princípios que deverão ser observados por todos os agentes de tratamento de dados ao realizar quaisquer ações, desde a coleta até o descarte.

São eles: (i) a finalidade, (ii) a adequação, (iii) a necessidade, (iv) o acesso livre, (v) a qualidade dos dados, (vi) a transparência, (vii) a segurança, (viii) a prevenção, (ix) a não-discriminação e (x) a responsabilização do agente.

A partir do estudo desses princípios, que tem como objetivo a proteção aos dados pessoais e regulamentação do tratamento destes, é possível perceber o quão sensível é o assunto e a sua importância, sendo plausível a ideia de eleva-lo ao *status* de direito fundamental.

É preciso ter noção de que tratar de dados pessoais é semelhante ao tratar do direito à privacidade e da personalidade de cada indivíduo, é perceber a autonomia deste direito.

A base e o início de todo recolhimento de dados é o consentimento, o titular precisa consentir livre e expressamente que permite o recolhimento de seus dados para a finalidade que

[8] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

fora exposta a ele.[9] Assim, o princípio da finalidade visa que os dados pessoais não sejam recolhidos para finalidade diversa da informada no momento do recolhimento.

Entretanto, há exceções previstas na lei para que se possa ser utilizado os dados para a finalidade diversa da que fora informado. Essas exceções são (i) para o cumprimento de uma obrigação legal por parte do controlador; (ii) para a execução do contrato que subsiste entre as partes; (iii) para o exercício regular do direito de ação; (iv) para a proteção da vida do titular ou de terceiros; (v) legitimo interesse do controlador e, por fim (vi) para proteção ao crédito.

O princípio da adequação, intimamente ligado ao princípio da finalidade é justamente a compatibilidade do tratamento de dados para a finalidade informada, conforme consentimento dado pelo titular. É a exata adequação do que fora informado pro titular no momento de recolhimento do dado ao que é de fato usado.[10]

A necessidade disposta como princípio nada mais é do que a limitação ao mínimo necessário ao realizar o tratamento dos dados, é da garantia de que não será recolhido nenhum dado sobressalente, sendo tratado e armazenado apenas dados necessários a atingir a finalidade para a qual fora consentido.[11]

---

[9] PINHEIRO, Patrícia. Conceitos e terminologias. In: PINHEIRO, P. P. **Proteção de dados pessoais - comentários à Lei n. 13.709/2018 LGPD.** São Paulo: Saraiva Educação, 2018. p. 33.

[10] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

[11] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

O livre acesso é a forma de garantir o direito ao titular dos dados de ter total e livre acesso aos seus dados que estão armazenados por outros. Não apenas o acesso, mas um acesso fácil, gratuito e total a todos os seus dados.

O acesso a forma como esses dados serão utilizados e por quem, está garantido pelo princípio da transparência, respeitado o segredo comercial da empresa que deverá ser resguardado.[12] A transparência visa garantir ao titular total conhecimendo do porquê e para quê seus dados estão sendo coletados.

Também posto como um princípio mas traduzido como um direito do titular, é a qualidade dos dados tratados pelas outras pessoas. Não são todos os tipos de dados que são considerados dados pessoais, precisam ser dados objetivos acerca de uma determinada pessoa.

Ou seja, é garantir que seus dados serão corretos, claros e da possibilidade de poder atualiza-los conforme haja mudanças. Afinal os dados pessoais são capazes de identificar uma pessoa na multidão, é necessário garantir que esses dados irão corresponder ao seu titular.[13]

É possível entender a importância desse princípio quando pensamos em algo negativo. Se a sua imagem está ligada a pedofilia, ao racismo, a algo pejorativo, é importante que seja um direito seu de alterar tal informação.

---

[12] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

[13] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

Os outros princípios podem ser traduzidos como os deveres do controlador de dados para com os titulares dos dados. O princípio da segurança nada mais é que a utilização de medidas técnicas e administrativas para proteger os dados pessoais.

É buscar mecanismos de seguranças a fim de salvaguardar os titulares de dados, não sendo aceitável um mecanismo retrógrado, falho e passível de alterações por qualquer pessoa.

O princípio da prevenção, embora possa parecer pelo nome impossível de ser alcançado, não é da obrigatoriedade do controlador em prevenir todo e qualquer incidente de segurança, mas de se precaver, adotando medidas a fim de evitar ao máximo esses incidentes.[14]

A responsabilização e prestação de contas pelo controlador é definida com clareza seu objetivo no art. 6º, inciso X: "responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".[15]

A não discriminação, por fim, é um princípio que já há na nossa constituição, ditas em outras palavras pelo art. 3º, inciso IV[16], que é um objetivo fundamental do nosso país promover o bem de todos sem qualquer discriminação.

---

[14] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

[15] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

[16] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em:

> Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil:
>
> IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.

Assim, os dados não deverão ser utilizados para fins discriminatórios ou ilícito. Esse princípio demonstra a clara necessidade da elevação da proteção de dados à um direito fundamental, pois os dados descrevem fielmente seu titular, devendo ser protegido tal como a sua personalidade.

Os princípios específicos da proteção de dados pessoais definidos nessa lei brasileira têm sua importância fundamental pelo fato de se tornarem vetores para a consecução da proteção de dados. Não são apenas princípios doutrinários para a explicação de algum instituto, são princípios expressos em lei que visam um objetivo.[17]

4 A PROTEÇÃO DE DADOS COMO UM DIREITO FUNDAMENTAL

Conforme demonstrado nos capítulos anteriores, a sensibilidade do tratamento de dados merece atenção diferenciada e não apenas pode-se aceitar que a proteção de dados seja uma mera extensão do direito à privacidade ou da personalidade.

Os dados são capazes de identificar não apenas o seu titular mas toda a sua vida, seus hábitos, seus gostos e desgostos, o uso dos dados são amplamente utilizados para converter vendas, por exemplo, pois a partir da coleta dos dados, são apresentados anúncios que coincidem com o gosto do titular.

<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

[17] RUARO, R. L. A TENSÃO ENTRE O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E O LIVRE MERCADO. REPATS - Revista de Estudos e Pesquisas Avançadas, Brasília, v. 4, n. 1, p. 389-423, Jan-Jun 2017. P.409.

Isso transcende a uma mera expansão dos direitos de privacidade e da proteção já existente aos direitos de personalidade, demonstrando a sua clara autonomia frente a esses direito.

Os riscos intrínsecos a atividade de tratamento automatizada de dados coloca em pauta a necessidade da criação de um novo direito fundamental para que seja constitucionalmente protegido e buscado. Nas palavras de Danilo Doneda:

No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada[18]

Ou seja, o avanço tecnológico impulsiona o avanço legislativo e suplica por uma mudança constitucional a fim de proteger esse assunto tão recente que já evidencia perigos eminentes. É impossível garantir uma proteção tecnológica blindada, entretanto é essencial que se garanta mecanismo para garanti-la.

Não é tão raro a expressão "dados são o novo petróleo" e tal como a extração de petróleo é regida por duras leis a fim de evitar o desgaste ambiental por ser um interesse coletivo, os dados carecem de proteção individualizada a fim de evitar uma afronta ao princípio da dignidade humana.

Outro fator que evidencia a autonomia da proteção de dados é o fato de já ter princípios próprios e específicos dispostos na Lei

[18] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, v. 12, n. 2, 2011. p. 103

Geral de Proteção de Dados. Com a autonomia, se faz necessário a sua configuração em um direito fundamental e diferente de alguns princípios que são tidos como indiretos, a proteção de dados precisa estar expressa para que se mude toda uma cultura em prol de alcançar a proteção de dados.[19]

O direito à proteção de dados poderá ser classificado como um novo direito da personalidade, que a integra mas não que já faz parte dos existentes. É imperioso reconhecer sua criação para que assim haja ampliação normativa para que não ocorra uma confusão entre as leis já existentes.[20]Bruno Bioni define:

> O direito à proteção dos dados pessoais deve ser alocado como uma nova espécie do rol aberto dos direitos da personalidade, dando elasticidade à cláusula geral da tutela da pessoa humana. Caso contrário, corre-se o risco de ele não se desprender das amarras conceituais e da dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana[21]

4.1 Bases legais: do consentimento à proteção de crédito como garantia a eficácia do direito à proteção de dados

Seguindo nessa mesma linha, além de elevar o direito a proteção de dados à um direito fundamental, importante é garantir a sua plena eficácia. A autodeterminação informacional pelo consentimento é a forma mais limpa e fácil de se conseguir alcança a plena eficácia da proteção aos dados como direito fundamental.

---

[19] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, v. 12, n. 2, 2011. p. 101

[20] BIONI, Bruno. Dados Pessoais e Direito da Personalidade *in:***Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. ed. Rio de Janeiro: Forense, 2020. p.92

[21] BIONI, Bruno. Dados Pessoais e Direito da Personalidade *in:***Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. ed. Rio de Janeiro: Forense, 2020. p.94

O consentimento definido na lei geral de proteção de dados em seu art. 5º, inciso XII, define novos rumos, agora o titular precisa que seu aval seja manifestado de forma livre, sem que haja imposição para isso, que ele seja devidamente informado para qual finalidade está dispondo de seus dados e de forma inequívoca, sem qualquer indução ao erro.[22]

Isso gera toda uma mudança da cultura atual, podendo ser exemplificada nos termos de uso de qualquer site com o "li e concordo" que durante os anos, era tão raro que alguém de fato lesse, que algumas empresas inclusive colocam entre eles premiações para quem de fato lesse e enviasse um e-mail requerendo o prêmio.

Um caso que ficou famoso fora o da empresa *Gamestation* em que nos seus termos colocou a cláusula que quem clicasse no "li e concordo" estaria vendendo sua alma para o dono da empresa, cerca de 7,5 mil pessoas aceitaram.[23]

Observando essa postura de grande parte da população e da crescente importância dos dados pessoas, o consentimento tivera que ser repensado e reformulado, as empresas assim que a LGPD entrar em vigor precisarão atualizar suas políticas internas e principalmente alterar a forma como coleta os dados de seus titulares.

A autodeterminação nesse sentido é alcançada graças a esse novo consentimento. É preciso garantir ao titular a possibilidade de

[22] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 01 jun. 2020.

[23] ARRUDA, Felipe. Contrato de licença: concordou e não leu, sua alma você vendeu. **Tecmundo**, 2011. Disponivel em: <https://www.tecmundo.com.br/consumidor/10206-contrato-de-licenca-concordou-e-nao-leu-sua-alma-voce-vendeu.htm>. Acesso em: 01 jun 2020.

determinar quais serão os seus dados a serem coletados, como eles serão tratados e para qual finalidade.[24]

Essa autodeterminação informativa visa resguardar o titular dos dados contra a utilização indevida de suas informações, evitando a discriminação e assegurando o respeito à dignidade da pessoa humana.[25]

A garantia de que todo o tratamento de dados atenda a sua legitima expectativa ou seja, que cumpra exatamente a sua finalidade, é garantir a proteção a esse direito, sendo ele já definido como direito fundamental ou seja apenas como um direito positivado em lei complementar.[26]

Válido ressaltar que o consentimento aqui definido é uma das bases legais definidas no art. 7º da LGPD, havendo outras bases legais que legitimam a coleta de dados, entretanto, são bases legais que respeitam ideais necessários de serem garantidos tal como a autodeterminação para que não haja um impacto econômico.

Se fosse possível apenas a coleta de dados por meio do consentimento, é notório que diversas empresas iriam falir, tal como o petróleo, é necessário que seja regulamentada a sua extração e não proibida.

As outras bases legais são (i) para cumprimento de obrigação legal ou regulatória pelo controlador, (ii) pela administração

[24] BIONI, Bruno. Leis setoriais e a Lei Geral de Proteção de dados pessoais *in*: **Proteção de dados pessoais: a função e os limites do consentimento.** 2. ed. ed. Rio de Janeiro: Forense, 2020. p.129

[25] RUARO, R. L. A TENSÃO ENTRE O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E O LIVRE MERCADO. REPATS - Revista de Estudos e Pesquisas Avançadas, Brasília, v. 4, n. 1, p. 389-423, Jan-Jun 2017.p. 410

[26] BIONI, Bruno. Dados Pessoais e Direito da Personalidade *in:***Proteção de dados pessoais: a função e os limites do consentimento.** 2. ed. ed. Rio de Janeiro: Forense, 2020. p.104

pública para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou devidamente respaldadas, (iii) para a realização de estudos por órgãos de pesquisas, (iv) para execução de contrato, (v) para o exercício regular do direito de ação, (vi) para a proteção da vida, seja do titular ou de terceiros, (vii) para tutela da saúde, (viii) legítimo interesse do controlador e (ix) para a proteção do crédito.

A lei definiu bases legais o suficiente para garantir a eficácia da proteção de dados. Se fosse apenas com base no consentimento, seria impossível que alguém entrasse com um processo contra outra, pois não poderia utilizar nenhum de seus dados e seria impossível sua intimação.

Autorizar o uso dos dados para estudos é garantir o avanço no seara das pesquisas, afinal, são precisos coletar dados para desenvolver estatísticas e mostrar para que rumo seguir.

A coleta de dados para a proteção da vida e da tutela da saúde estão acima de qualquer direito particular de autodeterminação. É a garantia do direito à vida e a saúde não apenas do titular dos dados, mas de toda a sociedade. Isso pode ser embasado no contrato social de Rousseau, pois no pacto social as pessoas abrem mão de determinados direitos em prol do estado que visa o bem estar social.[27]

O legitimo interesse é, de fato, a base legal mais discutida e também a mais difícil de ser utilizada. Por isso, é necessário que antes que um controlador decida coletar dados utilizando-se desta

[27] PISSURNO, Fernanda. O contrato social. **InfoEscola**, 2010. Disponivel em: <https://www.infoescola.com/livros/o-contrato-social/>. Acesso em: 01 jun 2020.

base legal, que ele faça o teste LIA. Esse teste visa balancear os direitos em jogo, o do interesse legítimo e a legítima expectativa.[28]

O art. 10º da LGPD embasa esse teste que consiste em (i) primeiramente verificar se o interesse do controlador não contraria outros dispositivos legais e se essa coleta de dados irá gerar vantagens ao controlador e nenhuma ao titular; (ii) averiguar a necessidade dessa coleta de dados e se condiz com a vantagem que o controlador irá obter sempre coletando o mínimo necessário; (iii) balanceamento, ou seja, se já há uma expectativa do titular em ter esses dados coletados por esse controlador.[29]

Por fim, não é uma etapa do teste mas sim uma obrigação ao utilizar-se dessa base legal, é de dar a possibilidade ao titular de se opor a essa coleta, é sempre ser transparente e dar a possibilidade de ter seus dados excluídos e não mais participar dessa coleta.[30]

Assim, é possível verificar que todas as bases legais são uma forma de garantir a proteção de dados e que cada uma deve ser utilizada para a sua finalidade, não podendo ter um uso irresponsável delas sem qualquer discernimento.

Ao realizar o tratamento de dados, será necessário uma pessoa que saiba com o que está lidando e isso se dará por meio da fiscalização da Autoridade Nacional de Proteção de Dados que

[28] BIONI, Bruno. A reavaliação substantiva (conteúdo) do consentimento como protagonista da proteção de dados pessoais *in:***Proteção de dados pessoais: a função e os limites do consentimento.** 2. ed. ed. Rio de Janeiro: Forense, 2020. p.234

[29] BIONI, Bruno. A reavaliação substantiva (conteúdo) do consentimento como protagonista da proteção de dados pessoais *in:***Proteção de dados pessoais: a função e os limites do consentimento.** 2. ed. ed. Rio de Janeiro: Forense, 2020. p.236

[30] BIONI, Bruno. A reavaliação substantiva (conteúdo) do consentimento como protagonista da proteção de dados pessoais *in:***Proteção de dados pessoais: a função e os limites do consentimento.** 2. ed. ed. Rio de Janeiro: Forense, 2020. p.238

não poderá ignorar as falhas e deverá aplicar as sanções previstas na lei.

5 CONCLUSÃO

Por todo o demonstrado é plenamente possível chegar-se a conclusão de não apenas ser necessário a proteção de dados ser considerada um direito fundamental, mas de que isso é um apelo feito pelas evoluções tecnológicas que a sociedade passou e passa todos os dias.

Entender o seu caráter autônomo frente aos demais direitos fundamentais e garantir sua plena eficácia e aplicação para resguardar a sociedade, dando total aplicabilidade aos seus direitos e a LDPG que entrará em vigor.

A falta de uma proteção constitucional e o não reconhecimento deste direito como fundamental coloca em risco toda a sociedade pois a sua proteção é diretamente o resguardo dos cidadãos que compõe toda a sociedade.

Observada essa necessidade é preciso entender que é um direito autônomo pela sua importância, não podendo ser apenar uma extensão de outros para que seja garantida uma proteção total.

Essa proteção, por sua vez, precisa ser garantida e eficaz, sendo inútil a sua mera declaração. Tal proteção e efetiva garantia do direito fundamental a proteção de dados poderá ser feita por meio da autodeterminação informacional com base no consentimento do titular de dados.

O consentimento não poderá ser o consentimento viciado que temos nos famigerados "li e concordo", deverá ser dado de forma livre, inequívoco e especifico para o fim que foi pedido, forçando

uma mudança cultural e estrutural não apenas nos coletores de dados, mas nos dos titulares em cobrarem uma postura correta ao tratar seus dados.

De igual forma, é inaceitável que se faça uma vista grossa com o uso da base legal do legitimo interesse, é preciso que o órgão de proteção dos dados pessoas fiscalize e aplique as sanções previstas para quem não fizer o teste de proporcionalidade LIA.

Essa base legal precisa ser garantida com um uso estrito e excepcional e não como uma brecha para que continue como está hoje, com a coleta de dados de forma desenfreada e em massa.

Para garantir a plena eficácia da proteção aos direitos pessoais é necessário que sejam respeitadas as bases legais para a coleta dos dados pessoais, não podendo mais ser aceita a coleta demasiada e sem objetivos.

REFERÊNCIAS

ARRUDA, Fernanda. Contrato de licença: concordou e não leu, sua alma você vendeu. **Tecmundo**, 2011. Disponivel em: <https://www.tecmundo.com.br/consumidor/10206-contrato-de-licenca-concordou-e-nao-leu-sua-alma-voce-vendeu.htm>. Acesso em: 01 jun 2020.

BIONI, Bruno. A reavaliação substantiva (conteúdo) do consentimento como protagonista da proteção de dados pessoais *in:***Proteção de dados pessoais: a função e os limites do consentimento.** 2. ed. ed. Rio de Janeiro: Forense, 2020. p 230-238.

BIONI, Bruno. Dados Pessoais e Direito da Personalidade *in:***Proteção de dados pessoais: a função e os limites do consentimento.** 2. ed. ed. Rio de Janeiro: Forense, 2020. p.104

BIONI, Bruno. Leis setoriais e a Lei Geral de Proteção de dados pessoais *in*: **Proteção de dados pessoais: a função e os limites do consentimento.** 2. ed. ed. Rio de Janeiro: Forense, 2020. p.129

BIONI, B. R. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. ed. Rio de Janeiro: Forense, 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**, ago 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 mai 2020.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, v. 12, n. 2, p. 91 - 108, 2011.

PINHEIRO, P. P. Conceitos e terminologias. In: PINHEIRO, P. P. **Proteção de dados pessoais - comentários à Lei n. 13.709/2018 LGPD**. São Paulo: Saraiva Educação, 2018. p. 25.

PISSURNO, F. P. O contrato social. **InfoEscola**, 2010. Disponivel em: <https://www.infoescola.com/livros/o-contrato-social/>. Acesso em: 01 jun 2020.

RUARO, R. L. A TENSÃO ENTRE O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E O LIVRE MERCADO. **REPATS - Revista de Estudos e Pesquisas Avançadas**, Brasília, v. 4, n. 1, p. 389-423, Jan-Jun. 2017.

O MARCO CIVIL DA INTERNET E A QUEBRA DO SIGILO DOS REGISTROS

Lucas Coutinho Borin[1]

RESUMO

O uso da internet é uma necessidade humana na atualidade. Hodiernamente, seu uso cresce exponencialmente na sociedade, principalmente em razão da possibilidade de facilitar a propagação de informações e a comunicação pessoas fisicamente distantes, sendo inclusive motivo para estarrecimento quando um indivíduo se priva de seu uso ou de usar determinados conteúdos, como as redes sociais. Em razão da facilidade que a internet possui em propagar informações, é necessário que exista uma regulamentação jurídica para estabelecer direitos e deveres, com o intuito de resguardar a vida privada aqueles que utilizam o meio digital, evitando que sejam aviltado no uso da internet. Busca-se, portanto, estudar a Marco Civil da Internet, legislação esta que inovou na ordem jurídica estabelecendo normas para assegurar os direitos dos usuários nos meios digitais, de forma prática e teórica.

Palavras-chave: Internet. Direitos. Responsabilidade.

ABSTRACT

The internet usage is a human need nowadays. Today, its usage has increase exponentially in the society, especial because the easiness to spread information e to allow distant people to communicate with themselves, even being a reason to dismay when someone do not use the internet or its contend. Due to this

[1] Aluno da pós graduação em Direito do Instituto Ceub de Pesquisa e Desenvolvimento – ICPD/UniCEUB.

facility to spread information, make it necessary to the Govern to regulate the user's rights and duties, regarding the intimacy to those who use the digital word, avoiding them demean on the internet. This article studies the Marco Civil da Internet, a new legislation that innovated in Brazilian's laws by establishing rights to internet users, using some theoretic and practical ideas.

Keywords: Internet. Rights. Responsibility.

1 INTRODUÇÃO

O Direito Penal passou por diversas fases durante a história. Os conceitos de crime sofreram diversas mudanças, bem como as espécies de sanções penais a serem aplicadas, passando por diversas fases como a Lei de Talião, até chegarmos ao atual Direito Penal do Fato.

Os tipos penais sofreram mutações ao longo da história, passando a determinadas condutas deixarem de ser ilícitas (*v.g.*, o adultério) em decorrência da ausência de interesse da sociedade em mantê-las como crime. Outras, contudo, foram tipificadas com o intuito de tutelar os interesses sociais que hodiernamente vem sendo alterado conforme os avanços da humanidade, sendo como exemplo o art. 154-A acrescido ao Código Penal pela Lei nº 12.737, de 30 de novembro de 2012, o qual tutela os dados e informações pessoais que se encontram dentro de dispositivo informático.

Em razão do avanço exponencial da tecnologia, o Direito necessitou regular as relações jurídicas com o intuito de assegurar os direitos dos usuários, dando-lhes ampla proteção, desde a preservação de seus dados contra terceiros à concessão de tutelas judiciais com o intuito de preservar provas para posterior responsabilização do infrator.

Fora em razão da necessidade de um regulamento jurídico que se editou a Lei nº 12.965, de 23 de abril de 2014, conhecida como o Marco Civil da Internet, trazendo ao ordenamento jurídica a norma processual prevista no art. 22 possibilitando a requisição de registros pelos ofendidos, cujo intuito é a preservação de provas e viabilizar elementos suficientes para intentar ação judicial apurando a responsabilidade dos infratores.

Ante o exposto, definiu-se o objeto de estudo do presente trabalho a tutela judicial prevista no art. 22 da Lei nº 12.965/14, a ser estudada de forma teórica e prática.

2 A PROTEÇÃO DOS DADOS DO USUÁRIO NO MARCO CIVIL DA INTERNET E NA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei nº 12.965/14, conhecida como Marco Civil da Internet, teve como principal objetivo regulamentar os fatos jurídicos ocorridos no âmbito da internet, assegurando diversos deveres e garantias às pessoas jurídicas que exploram a empresa pela internet ou a internet (caso dos provedores de conexão) e às pessoas jurídicas ou físicas que utilizam os conteúdos disponíveis na internet.

2.1 A Motivação da Lei Nº 12.965/14

A Lei nº 12.965/14 fora apresentada ao Congresso Nacional em 2011 pelo Chefe do Poder Executivo, tornando-a no Projeto de Lei nº 2.126. Transformou-se em lei ordinária e fora publicada em 23 de abril de 2014, tem como principal objetivo estabelecer princípios, garantias e deveres ao uso da internet no Brasil.

Segundo explicitado no teor do Projeto de Lei nº 2126/2011, a lei fora fruto do anteprojeto desenvolvido pela Secretaria de

Assuntos Legislativos do Ministério da Justiça - SAL/MJ em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas do Rio de Janeiro, buscou regulamentar o uso da internet em decorrência do crescente número de usuários.

Afere-se pela leitura da exposição de motivos do projeto, dois principais motivos para a elaboração do projeto de lei. O primeiro foi o intuito de preservar os usuários dos serviços, cujo intuito é o de vedar que agentes com maior poder econômico se imponham aos provedores de acesso, prejudicando os usuários. Neste sentido, cite-se o trecho da exposição de motivos: *"[...] a tendência do mercado é a de que os interesses dos agentes de maior poder econômico se imponham sobre as pequenas iniciativas, e que as pretensões empresariais enfraqueçam os direitos dos usuários."*

Não atoa que a lei assegurou tal direito em seu art. 7º, inciso VII, a vedação aos provedores de acesso de fornecer quaisquer dados de usuários a terceiros, salvo quando houver consentimento livre do usuário. A especial razão para tal proteção se encontra no fato de a sociedade moderna ser considerada como a sociedade da informação. Atualmente, a informação possui um valor econômico de alta relevância no mundo, em especial na internet. Quanto maior a informação que uma pessoa tem sobre a outra, mais o seu poder sobre ela.

O segundo motivo fora o de resguardar a responsabilidade dos provedores de acesso e de conteúdo quando houvesse a prática de um ato ilícito na internet. Na ocasião da apresentação do projeto, o estudo desenvolvido se assentou na seguinte premissa:

> Para o Poder Judiciário, a ausência de definição legal específica, em face da realidade

> diversificada das relações virtuais, tem gerado decisões judiciais conflitantes, e mesmo contraditórias. Não raro, controvérsias simples sobre responsabilidade civil obtêm respostas que, embora direcionadas a assegurar a devida reparação de direitos individuais, podem, em razão das peculiaridades da Internet, colocar em risco as garantias constitucionais de privacidade e liberdade de expressão de toda a sociedade.(CONGRESSO NACIONAL, 2011)

Ademais, não subsiste razão para responsabilizar os provedores que estão fornecendo um serviço por terceiro que se utiliza destes para praticar atos ilícitos em sentido amplo. Convém ressalte-se a regra do art. 29 do Código Penal, o qual estabelece que somente haverá concurso de agentes àquele que consentiu e concorreu para a prática do delito. Tal regra vem inserida no inciso VI do art. 3º da lei em comento, o qual afirma que haverá a "responsabilização dos agentes de acordo com suas atividades, nos termos da lei".

2.2 Os Conceitos Trazidos Pela Lei

Previstos no art. 5º, a lei conceituou dois dos principais registros nos incisos VI e VIII, assim expostos:

> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
>
> [...]
>
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Os registros de conexão são guardados pelos provedores de acesso, que consiste na pessoa jurídica que fornece o serviço de acesso à internet por meio da banda larga (LIMA, 2016).

Os registros de acesso a aplicações de internet são todas as informações guardadas pelos provedores de aplicações de internet, para os quais o art. 15 da Lei nº 12.965/14 conceituou como as pessoas jurídicas que exercem a atividade de serviços de aplicações de internet de forma organizada e com fins econômicos. Consiste, a título de exemplo, nas redes sociais como o Facebook e aplicativos como WhatsApp, também conhecidos como provedores de conteúdo.

Da leitura do art. 5º, vislumbra-se não existir qualquer menção ao registro de uso, consistente no registro das atividades de determinado usuário dentro dos conteúdos providenciados pelos provedores de aplicações de internet, pois, assim como se depreende a intenção da Lei nº 12.965/14 em preservar os direitos e garantias dos usuários, resguardou que não seria possível aferir certos dados pessoais, como por exemplo a transferência de dados entre usuários (LIMA, 2016).

Desta forma, só é possível aferir dados como o endereço de protocolo de internet (endereço IP, consistente em um código de identificação de cada computador), o tempo de conexão do usuário e o Cadastro de Pessoa Física do possuidor do endereço de IP. Os dados pessoais atenderam a um tratamento específico regulamentado pela Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados, a qual entrará em vigor em 3 de maio de 2021, se aprovada a Medida Provisória nº 959, de 29 de abril de 2020, pelo Congresso Federal.

Por fim, convém mencionar um estudo realizado pela Agência Nacional de Telecomunicações – ANATEL, na qual afirmou a necessidade e capacidade de os provedores de aplicações de internet deverão fornecer a "porta lógica de origem" quando

houver múltiplos indivíduos utilizando do mesmo endereço de IP. (ANATEL, 2014)

Ocorre que mesmo com o endereço de IP, quando compartilhado, não se é possível identificar e individualizar o usuário. Para a devida identificação é necessário, portanto, obter informação sobre a "porta lógica" ou porta de acesso, que demonstre a conexão do usuário com a internet e sua comunicação com outros terminais, compreendida como "porta lógica de origem". (ANATEL, 2014)

Ao julgar causa relacionada ao fornecimento de registros de conexão e de acesso a aplicações de internet, o Superior Tribunal de Justiça entendeu ser plenamente possível a determinação judicial para o fornecimento do endereço de IP, bem como a "porta lógica de origem". O aresto ficou assim ementado:

> RECURSO ESPECIAL. CIVIL E PROCESSUAL CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. PROVEDOR DE APLICAÇÕES. IDENTIFICAÇÃO DO DISPOSITIVO UTILIZADO PARA ACESSO À APLICAÇÃO. INDICAÇÃO DO ENDEREÇO IP E PORTA LÓGICA DE ORIGEM. INTERPRETAÇÃO TELEOLÓGICA DOS ARTS. 5º, VII, E 15 DA LEI N. 12.965/2014. RECURSO ESPECIAL PROVIDO.
>
> 1. O recurso especial debate a extensão de obrigação do provedor de aplicações de guarda e fornecimento do endereço IP de terceiro responsável pela disponibilização de conteúdo ilícito às informações acerca da porta lógica de origem associada ao IP.
>
> 2. A previsão legal de guarda e fornecimento dos dados de acesso de conexão e aplicações foi distribuída pela Lei n. 12.965/2014 entre os provedores de conexão e os provedores de aplicações, em observância aos direitos à intimidade e à privacidade.
>
> 3. Cabe aos provedores de aplicações a manutenção dos registros dos dados de acesso à aplicação, entre os quais se inclui o endereço IP, nos termos dos arts. 15 combinado com o art.

> 5º, VIII, da Lei n. 12.965/2014, os quais poderão vir a ser fornecidos por meio de ordem judicial.
>
> 4. A obrigatoriedade de fornecimento dos dados de acesso decorre da necessidade de balanceamento entre o direito à privacidade e o direito de terceiros, cujas esferas jurídicas tenham sido aviltadas, à identificação do autor da conduta ilícita.
>
> 5. Os endereços de IP são os dados essenciais para identificação do dispositivo utilizado para acesso à internet e às aplicações.
>
> 6. A versão 4 dos IPs (IPv4), em razão da expansão e do crescimento da internet, esgotou sua capacidade de utilização individualizada e se encontra em fase de transição para a versão 6 (IPv6), fase esta em que foi admitido o compartilhamento dos endereços IPv4 como solução temporária.
>
> 7. Nessa fase de compartilhamento do IP, a individualização da navegação na internet passa a ser intrinsecamente dependente da porta lógica de origem, até a migração para o IPv6.
>
> 8. A revelação das portas lógicas de origem consubstancia simples desdobramento lógico do pedido de identificação do usuário por IP.
>
> 9. Recurso especial provido.
>
> (REsp 1784156/SP, Rel. Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em 05/11/2019, DJe 21/11/2019)

2.3 A Responsabilidade Civil dos Provedores

Acertadamente a Lei nº 12.965/14 mitigou a responsabilidade de alguns dos provedores, prevendo casos específicos em que permite a responsabilização do provedor de aplicações de internet, previsto em seu art. 19, o qual afirma:

> 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.

No mesmo sentido, dispõe o art. 21 sobre a responsabilidade subsidiária dos provedores de aplicações de internet que disponibiliza conteúdo de terceiros que violam a vida privada do usuário. Neste sentido:

> 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.

A respeito dos provedores de acesso à internet, estabeleceu o art. 18 que não haverá quaisquer responsabilidades civis pelos conteúdos de terceiro.

A lei se estrutura em cinco capítulos a saber: disposições preliminares, direitos e garantias do usuário, provisão de conexão e de aplicações de Internet, atuação do poder público e disposições finais.

O primeiro capítulo disciplina, em seus arts. 2º ao 6º, os princípios aplicáveis ao uso da internet e apresenta conceitos sobre termos técnicos; o segundo capítulo trouxe em seus arts. 7º e 8º as garantias e direitos dos usuários; o terceiro capítulo fora dividido em IV seções regulando o tráfego de dados, o dever de neutralidade dos provedores de acesso, o dever de os provedores proteger os registros, aos dados pessoais, comunicações privadas, responsabilidade aos provedores pelos dados causados por

terceiros, a requisição judicial dos registros; o quarto capítulo dispõe sobre a atuação do poder público na internet, estabelecendo seus deveres, garantias e direitos; por fim, no quinta capítulo tem-se as disposições finais.

Vislumbra-se, portanto, como principal escopo da lei o de delimitar os deveres e responsabilidades a serem exigidos dos prestadores de serviços e define o papel a ser exercido pelo poder público em relação ao desenvolvimento do potencial social da rede. Tal proteção é encontrada em diversos outros artigos além dos supramencionados:

2.4 A Relação Entre a Lei Geral de Proteção de Dados e o Marco Civil da Internet

A principal intenção do legislador com o Marco Civil da Internet fora regular os fatos jurídicos ocorridos constantemente no âmbito da internet, assegurando normas jurídicas de proteção e de deveres a todos que usufruem do serviço.

Consoante o exposto acima, afere-se que a Lei nº 12.965/14 não tratou de forma específica sobre os dados pessoais, isso porque buscou resguardar de forma especifica os registros de acesso e conexão dos usuários. Por tal motivo, editou-se a Lei nº 13.709/18, tendo seu principal objetivo o tratamento de dados pessoais, inclusive no âmbito digital, cuja essência do ato normativa é o de proteger os direitos fundamentais da liberdade e da privacidade da pessoa natural, estabelecendo diretrizes para o tratamento de dados pessoais, isto é, qualquer técnica de manuseio de dados relativos ao indivíduo, em especial dos usuários. (PINHEIRO, 2018, p. 16)

Em razão da internet não possuir limites territoriais, sua aplicação não se termina apenas aos fatos ocorridos Brasil,

aplicando-se à todas pessoas naturais ou jurídicas que venham a tratar de dados fora do território nacional, desde que tais dados tenham sido obtidos no país. (PINHEIRO, 2018, p. 30)

Desta forma, a proteção que o Marco Civil da Internet não conferiu aos dados pessoais será obtida pela Lei nº 13.708/18, conhecida como Lei Geral de Proteção de Dados - LGPD, fazendo com que ambas acabem por se completarem.

3 A QUEBRA DO SIGILO DOS REGISTROS DO USUÁRIO

A regra é o sigilo dos registros de acesso aos conteúdos da internet e da conexão do usuário à internet, compreendido aqui também os dados pessoais a aplicações de internet. De maneira a não viabilizar a impunidade dos agentes que se utilizam da facilidade da internet para cometer delitos, os quais muitas vezes são realizados de maneira anônima em razão da facilidade de se atribuir uma identidade diferente, o legislador previu a possibilidade de uma medida judicial determinando aos provedores de acesso ou de conteúdo, que forneçam tais registros.

Desta forma, estabeleceu o art. 22 da Lei nº 12.965/14, *in verbis*:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Trata-se da possibilidade de o Poder Judiciário ordenar aos provedores os registros de conexão ou de registro de acesso do usuário que pratica ato ilícito na internet. A conceituação de tais registros vem esculpida nos incisos VI e VIII do art. 5º,

Dessarte, na leitura dos incisos II e III do art. 7º, evidencia-se a possibilidade da quebra do sigilo dos registros do usuário, *in verbis*:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> [...]
>
> 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;

3.1 Requisitos do Art. 22

Estabeleceu o legislador no parágrafo único do art. 22 alguns requisitos a serem observados pelo interessado sob pena de sua inadmissibilidade pelo juiz, *in verbis*:

> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
>
> I - fundados indícios da ocorrência do ilícito;
>
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
>
> III - período ao qual se referem os registros.

Por se tratar de medida excepcional e que determina a quebra de um dado pessoal do usuário, o primeiro requisito determina que o interessado demonstre tão somente neste primeiro momento a existência do *fumus commissi delicti* (a fumaça do cometimento do delito) ou *fumus boni iuris* (fumaça do bom direito), podendo ser, a exemplo, a ata notarial expedida pelo notário dando fé pública acerca de um registro na internet que demonstre a existência de um possível delito. Há um limite subjetivo ao pedido intrínseco ao primeiro requisito, somente

podendo recair sobre os agentes ou agentes que praticam a conduta. Se terceiro de boa-fé, que sem intenção alguma venha a ter conhecimento dos dados, não pode sofrer com a medida. É o caso dos terceiros que "curtem" as postagens do agente que pratica uma difamação em rede social.

Além da demonstração do *fumus commissi delicti*, é necessário apresentar uma motivação idônea pelo interessado que comprove a necessidade da determinação judicial como medida imprescindível para aferir a possível investigação ou responsabilização cível ou penal do agente. Se há outros meios de provas que comprovem o fato ou outros meios de obtenção destas provas, o requerimento deverá ser indeferido, servindo como uma espécie de "último caso", sob pena de transformar a requisição em algo inescrupuloso.

No último requisito, requereu o legislador que o interessado estabelecesse um determinado período de tempo a que se refere os registros, em observância aos princípios da proporcionalidade e razoabilidade, tendo em vista coibir um determinado aviltamento do usuário transgressor. Assim, se os fatos iniciaram no mês de janeiro de 2020 e terminaram no mês de março de 2020, somente poderá solicitar o registro relativos a esse período de tempo, sob pena de nulidade da decisão judicial.

Trata-se de requisitos de suma importância, pois a ausência destes implicará na inadmissibilidade da requisição pelo juiz. Instado a se manifestar, o Tribunal de Justiça do Mato Grosso do Sul decidira da necessidade de que o requerimento deverá contar cumulativamente todos os requisitos. O julgado ficara assim ementado:

> APELAÇÃO CÍVEL – AÇÃO DE OBRIGAÇÃO DE FAZER C/C INDENIZAÇÃO POR DANOS MORAIS –

> DISPONIBILIZAÇÃO DE DADOS PESSOAIS – REDE DE INTERNET – LEI DO MARCO CIVIL DA INTERNET (N. 12.965/2014) – REQUISITOS – NÃO PREENCHIDOS – AUTORIZAÇÃO NÃO CONCEDIDA – SENTENÇA REFORMADA – RECURSO PROVIDO DO FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA. E IMPROVIDO DA SENAI. A sentença merece ser reformada, pois apesar da Lei n. 12.965/2014, em seu artigo 10, § 1º, autorizar a disponibilização de dados pessoais ou outras informações que possam contribuir para a identificação do usuário ou do terminal, sua apresentação somente ocorrerá se presente os requisitos do artigo 22 da referida lei. Após analisar os autos, constato que estão ausentes todos os requisitos legais que autorizam a quebra do sigilo de dados pessoais, quais sejam:fundados indícios da ocorrência do ilícito; justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e período ao qual se referem os registros. Destarte, se não estão preenchidos os requisitos estampados no artigo 22, parágrafo único e incisos, resta inviabilizado o pedido da requisição dos dados pessoais.
>
> (TJMS. Apelação Cível n. 0809642-63.2014.8.12.0001, Campo Grande, 1ª Câmara Cível, Relator (a): Des. Divoncir Schreiner Maran, j: 15/03/2016, p: 17/03/2016) (Ressalvam-se os grifos)

Ao se manifestar acerca do lapso de tempo dos registros, o Superior Tribunal de Justiça entendeu que somente deverá ser apresentado somente no caso de fluxo de comunicações (quando há transferência de dados) e quando se tratar de registros de aplicações de internet, definido no art. 5º, VII, como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet", sendo desnecessário que o autor aponte o período de tempo a que se referem os registros quando houver dados já armazenados, ou seja, em casos de dados estáticos. Neste sentido:

> RECURSO EM HABEAS CORPUS. OPERAÇÃO DI VENEZIA. ORGANIZAÇÃO CRIMINOSA LIGADA À

> EXPLORAÇÃO DE JOGOS DE AZAR. QUEBRA DE SIGILO TELEMÁTICO. LEI N. 12.965/2014 - LEI DO MARCO CIVIL DA INTERNET. POSSIBILIDADE DE ACESSO AOS DADOS TELEMÁTICOS SEM A NECESSIDADE DE LIMITE TEMPORAL, PARA FINS DE INVESTIGAÇÕES CRIMINAIS. RECURSO IMPROVIDO.
>
> 1. A Lei do Marco Civil da Internet aplica-se às relações privadas, e o art. 10 desse estatuto tem previsão ampla da necessidade de tutela da privacidade de dados pessoais e do conteúdo de comunicações privadas. Além disso, ao tratar do acesso judicial, somente exige limitação temporal no acesso aos registros de "aplicações de internet", termo legal usado para definir "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet" (art. 5°, VII).
>
> 2. Apesar de o artigo 22, III, da Lei n. 12.965/2014 determinar que a requisição judicial de registro deve conter o período ao qual se referem, tal quesito só é necessário para o fluxo de comunicações, sendo inaplicável nos casos de dados já armazenados que devem ser obtidos para fins de investigações criminais.
>
> 3. Recurso em habeas corpus improvido.
>
> (RHC 117.680/PR, Rel. Ministro NEFI CORDEIRO, SEXTA TURMA, julgado em 11/02/2020, DJe 14/02/2020) (Ressalvam-se os grifos)

Depreende-se do entendimento acima que somente será necessário apresentar o período de tempo quando se tratar de pessoas jurídicas que disponibilizam conteúdos na internet, tais como o Facebook e WhatsApp.

Os requisitos estipulados no parágrafo único são limites objetivos impostos ao pedido de requisição dos registros, e são cumulativos, exigindo a presença de todos eles na requisição, sem os quais deverá o juiz determinar a emenda da petição inicial para que o autor apresente-os sob pena de extinção do processo sem resolução de mérito nos termos do inciso I do art. 485 do Código de Processo Civil.

Ademais, convém ressaltar que o entendimento do Superior Tribunal de Justiça é no sentido de que o mero fornecimento do endereço de *IP* é suficiente para a identificação dos usuários, consoante a decisão exarada pela Ministra Maria Isabel Gallotti no Recurso Especial nº 1.865.325/PR. O julgado se torna mitigado quando houver compartilhamento de endereço de IP, razão pela qual o juiz poderá determinar o fornecimento também da "porta lógica de origem", consoante assentado no julgamento do Recurso Especial nº 1.784.156/SP de relatoria do Ministro Marco Aurélio Bellizze.

Consoante o disposto no art. 11 da Lei nº 13.709/18, é possível compreender que o tratamento de dados pessoais sensíveis[2] sem o consentimento do titular para fins de instrução processual, poderá observar os requisitos acima. Desta forma, o autor da ação deverá apontar o *fumus comissi delicti* ou *fumus boni iuris*, o porquê de os dados pessoais serem imprescindíveis para a investigação ou para a instrução do processo, bem como o período que tais dados se referem. Logo, é possível ao juiz a exemplo de uma investigação relativa a um sindicato que esteja desviando verbas, poderá determinar a quebra do sigilo de transferência de dados entre as pessoas envolvidas.

Em razão do entendimento consolidado no Superior Tribunal de Justiça, tal medida deverá ser residual, isto é, qual o fornecimento do endereço de *IP*, não consegue identificar corretamente os envolvidos na prática do ilícito.

[2] Relativo a dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, conforme conceituado pelo art. 5º, II, da LGPD.

3.2 Competência Para Concessão

Pela leitura do artigo em comento e para maior efetivação e garantia dos direitos individuais previstos na Constituição Federal, a quebra dos sigilos imprescinde de autorização judicial. Permite-se, portanto, tanto ao juízo criminal quanto ao cível estipular tais quebras. Tal afirmação é extraída da norma do art. 22 da lei em comento, a qual deverá ser lida junto com os incisos II e III do art. 7º, o qual trata dos direitos dos usuários.

Serão legitimados para propor a requisição: o usuário ofendido, o membro do Ministério Público e a autoridade policial. Esta última somente será legitimada para requerer a quebra do sigilo para os devidos fins de investigação.

A competência jurisdicional para a requisição judicial dos registros deverá observar as competências estabelecidas na Constituição Federal. Assim, tratando-se de crime cometido contra a União, *v.*g, a competência para a requisição dos registros será da Justiça Federal, sob pena de incompetência absoluta.

3.3 Do Procedimento

Da leitura do art. 22, depreende-se existir dois tipos de procedimentos diferentes: um autônomo, cujo principal objetivo é o de somente produzir provas, e um incidental, no qual produzirá as provas e em seguida será concedido o prazo para aditar a peça inicial (queixa-crime ou petição inicial, a depender do juízo).

O procedimento no juízo cível seguirá o comum ou sumaríssimo (no caso de juizado especial cível), onde deverá ao autor requerer incidentalmente o registro do usuário formalizando na petição causa de pedir para uma eventual indenização. Após a citação, caberá ao provedor apresentar contestação ou os

registros. Uma vez apresentado os registros e sendo possível identificar o agente, o juiz determinará a inclusão deste no processo e sua citação, seguindo-se com o procedimento comum previsto no Código de Processo Civil.

Por sua vez, no procedimento autônomo caberá ao advogado ajuizar a respectiva ação em face do provedor competente para fornecer os registros. O provedor será citado para apresentar os registros ou contestar, alegando qualquer matéria de defesa. Ao término, deverá o autor emendar a inicial para apresentar pedido de responsabilização do agente que cometeu o ato ilícito, bem como mover a ação em face dele, excluindo, desde já, o provedor do polo passivo.

Entendimento já pacificado pela jurisprudência e pela doutrina, tendo em vista as disposições contidas na lei as quais permite a concessão de liminar, faz-se possível a concessão de tutela de urgência de natureza antecipada ou cautelar. A Lei 12.965/14, estabelece em seu art. 13 que os provedores de conexão deverão manter os registros de conexão pelo prazo de 1 (um) ano. Desta forma, é possível requer a tutela de urgência para assegurar que tais registros não sejam deletados.

No mesmo sentido, tem-se o art. 15 para o qual se estabelece o dever de os provedores de aplicação de internet guardar os registros dos usuários pelo máximo de 6 (seis) meses.

Em razão das condições da ação ser diferente no processo penal, requerendo o lastro mínimo de autoria e materialidade para o prosseguimento da ação penal, deve-se entender que o procedimento no juízo criminal para fins de obtenção dos registros de conexão e de acesso somente será viável para fins de investigação criminal, não sendo possível ao ofendido, quando se

tratar de crime que se procedem mediante queixa-crime (ação penal privada), instaurar procedimento judicial para obtenção de conteúdo probatório.

Desta forma, só é possível à vítima do art. 140, *v.g*, intentar a queixa-crime quando possuir provas de autoria e materialidade. Poderá, portanto, se valer dos procedimentos cíveis com o escopo de identificar o autor do delito, sendo que o prazo decadencial para o exercício do direito da ação é de 6 meses a contar do conhecimento da autoria, conforme exposto pelo art. 38 do Código de Processo Penal.

4 DA REQUISIÇÃO DAS INFORMAÇÕES NOS JUIZADOS ESPECIAIS

Incentivando a celeridade processual, o legislador possibilitou ao ofendido recorrer ao rito sumaríssimo do juizado especial ao estabelecer os § 3º do art. 19, assim expostos:

> Art. 19. (...)
>
> § 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.

Da leitura dos dispositivos acima, verifica-se clara compatibilidade dos juizados especiais para julgar os processos de indenização em face do usuário transgressor da norma jurídica. Ademais, a leitura dos parágrafos acima deverá ser feita junto com o art. 22, retratada no capítulo 3 deste trabalho.

Instituído pela Lei nº 9.099, de 26 de setembro de 1995, conhecida como a Lei dos Juizados Especiais, fora editada para dar

eficácia à norma constitucional prevista no inciso I do art. 98 da Constituição Federal.

Para dar eficácia, institui-se alguns limites materiais para o reconhecimento do direito em postular perante tais juízos, sendo os mais importantes para o presente trabalho: a) o valor da causa não exceda 40 salários-mínimos (60 quando se tratar de juizados especiais federais e da fazenda pública), estabelecido no inciso I do art. 3º; e b) infrações penais não superiores a 2 anos, previsto no art. 61.

Desta forma, na ocorrência de um crime de difamação em rede social, é plenamente possível ajuizar uma ação no juizado especial criminal, requisitando incidentalmente os registros do usuário com o intuito de fomentar o conteúdo probatório. Contudo, a mesma lógica não se aplica quando, *v.g*, o agente pratica três vezes a infração do art. 138 em concurso material, na qual tornará o juizado especial criminal incompetente para o julgamento da causa.

Em razão de o procedimento processual ser mais célere, vislumbra-se ser mais adequado ao ofendido se utilizar dos juizados especiais cíveis e criminais, quando atendido os requisitos especificados acima, permitindo-o obter com mais facilidade e celeridade indenização decorrente do ilícito suportado.

Ademais, perfeitamente compatível a concessão de liminar antecipando os efeitos da tutela também no juizado especial, em decorrência da norma permissiva do §4º do art.19[3].

[3] § 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.

5 CONCLUSÃO

Ante o exposto no presente trabalho, conclui-se a Lei nº 12.965/14 tratou escorreitamente as relações jurídicas ocorridas nos meios digitais, resguardando os direitos fundamentais, em especiais os da vida privada e da intimidade, com o intuito de evitar o livre aviltamento dos usuários e a impunidade pelos danos causados a outrem.

O tratamento conferido pelo Marco Civil da Internet faz um paralelo com a Lei Geral de Proteção de Dados, isto porque ambos tem como principal escopo assegurar os direitos fundamentais da privacidade, sendo que o Marco Civil da Internet possui aplicação limitada aos meios digitais, enquanto a LGPD não encontra tal limitação. Ademais, é possível a comunicação de ambas leis ao tratar de uma relação jurídica.

Por se tratar de um direito inclusive considerado como fundamental na Constituição Federal, a quebra do sigilo dos registros somente poderá ser feito mediante requerimento ao Poder Judiciário, no qual deverá conter requisitos objetivos para seu deferimento, cujo intuito de tal limitação corrobora com o dever de assegurar os direitos e de tratar dignamente até mesmo o infrator de uma norma jurídica, caso contrário legitimaria o aviltamento deste.

Desta forma, com os requisitos apresentados ao juiz, será possível estabelecer dois procedimentos cíveis diferentes, incidental ou autônomo, enquanto no juízo criminal somente será possível solicitar o fornecimento dos registros pela autoridade policial ou pelo Ministério Público com o intuito de obter conjunto probatório suficiente para formar a *opinio delicti* do representante

do Ministério Público e para intentar ação penal em face do investigado.

Por fim, da leitura da Lei nº 12.965/14 é perfeitamente possível que tal requerimento seja encaminhada aos juizados especiais, inclusive para fins de responsabilização criminal, observando sempre os requisitos de competência estabelecidos na Lei nº 9.099/95. O autor do pedido poderá requerer tutela de urgência para a apresentação dos registros, inclusive nos juizados especiais.

REFERÊNCIAS

BRASIL. Congresso Nacional. Projeto de Lei nº 2.126, de 24 ago. 2011. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255. Acesso em: 3 jun. 2020.

_____. DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940. **Código Penal**, Rio de Janeiro, RJ, dez 1940. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm >. Acesso em: 2 out. 2018.

_____. DECRETO-LEI Nº 3.689, DE 3 DE OUTUBRO DE 1941. **Código de Processo Penal**, Rio de Janeiro, RJ, out 1941. Disponível em: < http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm>. Acesso em: 1 jun. 2020.

_____. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**, Brasília, DF, abr. 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 1 jun. 2020.

_____. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**, Brasília, DF, ago 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em: 1 jun. 2020.

_____. Superior Tribunal de Justiça (3. Turma). Recurso Especial. REsp 1784156/SP. Relator(a): Min. MARCO AURÉLIO BELLIZZE, 21 de novembro de 2019. Disponível em: https://ww2.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=REsp%201784156. Acesso em: 3 jun. 2020.

_____. Superior Tribunal de Justiça (4. Turma). Recurso Especial. REsp 1.865.325/PR. Relator(a): Min. MARIA ISABEL GALLOTTI, 30 de março de 2020. Disponível em: https://scon.stj.jus.br/SCON/decisoes/toc.jsp?processo=1865325.NUM.&b=DTXT&thesaurus=JURIDICO&p=true#DOC1. Acesso em: 24 maio 2020.

_____. Superior Tribunal de Justiça (6. Turma). Recurso em *Habeas Corpus*. RHC 117.680/PR. Relator(a): Min. NEFI CORDEIRO, 14 de fevereiro de 2020. Disponível em: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%28%22NEFI+CORDEIRO%22%29.MIN.&processo=117680&b=ACOR&thesaurus=JURIDICO&p=true. Acesso em: 24 maio 2020.

_____. Tribunal de Justiça do Mato Grosso do Sul. Apelação Cível n. 0809642-63.2014.8.12.0001. Relator(a): Des. Divoncir Schreiner Maran, 17 de março de 2016. Disponível em: https://esaj.tjms.jus.br/cjsg/resultadoSimples.do;jsessionid=1EDD328218EA74288573BE873D3EAE65.cjsg2?conversationId=&nuProcOrigem=0809642-63.2014.8.12.0001&nuRegistro=. Acesso em: 24 maio 2020.

GT-IPv6: Grupo de Trabalho para implantação do protocolo IPVersão 6 nas redes das Prestadoras de Serviços de Telecomunicações. Relatório Final de Atividades. 2014. Disponível em: https://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=325769. Acesso em: 3 jun. 2020.

LIMA, GLAYDSON DE FARIAS. Manual de direito digital: fundamentos, legislação e jurisprudência. 1. ed. Curitiba: Appris, 2016.

PINHEIRO, PATRICIA PECK. Proteção de Dados Pessoais: comentários à Lei n. 13.709/18 (LGPD). 1. ed. São Paulo: Saraiva, 2018.

A PROTEÇÃO DE DADOS E A TECNOLOGIA CRIPTOGRÁFICA: UM DUELO ENTRE O PODER PÚBLICO E A PRESERVAÇÃO DA PRIVACIDADE

Ana Carolina Vieira Freitas Lima[1]

RESUMO

O Brasil é o segundo país no mundo em número de crimes cibernéticos. Dados apontam que essa modalidade de crime é crescente em todo mundo, tendo em vista o aumento do uso da tecnologia. O roubo de dados pessoais dos usuários é uma das formas mais comuns do crime cibernético e atinge frontalmente a privacidade dos cidadãos. Nesse sentido, foi sancionada a Lei Geral de Proteção de Dados (Lei 13.709/18) . Essa lei surge para além da proteção de dados. Busca-se com ela a proteção da privacidade dos usuários, a transparência no uso dos dados pessoais, a adequação do desenvolvimento econômico e tecnológico à segurança da informação, de forma a reconhecer as tecnologias, como a criptografia, como aliados na segurando digital dos usuários.

Palavras-chave: Crimes cibernéticos. Proteção de dados. Criptografia.

ABSTRACT

Brazil is the second country in the world in number of cyber crimes. Data indicate that this type of crime is growing worldwide, in view of the increased use of technology. Theft of users 'personal

[1] Advogada. Graduada pelo Centro Universitário de Brasília – UniCeub. Aluna da pós-graduação *lato sensu* em Direito Público: Novas Tendências. Email:limacaroli@gmail.com.

data is one of the most common forms of cyber crime and directly affects citizens' privacy. In this sense, the General Data Protection Law (Law 13,709 / 18) was sanctioned. This law arises beyond data protection. It seeks to protect the privacy of users, transparency in the use of personal data, the adequacy of economic and technological development to information security, in order to recognize technologies, such as cryptography, as allies in users' digital holding.

Keywords: Cybercrimes. Data protection Cryptography.

1 INTRODUÇÃO

O presente artigo tem por objetivo analisar a utilização de dados pessoais para fins de investigação criminal. O uso da tecnologia na esfera penal visando melhorar os meios e as formas de investigação ganharam força nos últimos anos. É notório que a tecnologia está ocupando um espaço cada vez maior em qualquer área, mas no campo do Direito Penal ela ganhou bastante destaque. Isto ocorreu principalmente com o surgimento de novas tecnologias em smartphones, o que obrigou a adequação da persecução penal à nova realidade das informações.

Diante disso, percebe-se necessário entender que o impacto tecnológico demanda uma atualização constante do Direito. Deve-se até dizer que as pessoas continuam a serem detentora de direitos e deveres mesmo quando estão online, para que fique claro que uma internet segura é dever do Estado, e este não deve valer-se da insegurança dos cidadãos online para garantir o sucesso em outras demandas da segurança pública. É importante que a nova forma de condição das investigações criminais observe as garantias constitucionais e os direitos fundamentais dos cidadãos envolvidos nelas.

Diante do exposto, esse artigo buscará demonstrar a necessidade de se proteger os dados pessoais dos cidadãos, a

partir da conceituação de temas inerentes à proteção de dados pessoais e da sociedade da informação, em primeiro lugar. Após breve explanação, tratará das questões inerentes à criptografia, bem como os direitos à privacidade e ao sigilo das comunicações, observando os votos recentemente proferidos pelo Ministro Edson Fachin, na ADPF 403, e da Ministra Rosa Weber, na ADI 5527.

2 A SOCIEDADE DA INFORMAÇÃO E A PROTEÇÃO DE DADOS

2.1 Breves considerações e histórico

O tema da proteção de dados nunca foi tão atual. Com o avanço tecnológico surge a necessidade de se regular o ambiente virtual, isto é, a ciência jurídica se vê obrigada a acompanhar os novos desafios regulatórios trazidos por essa nova de sociedade.

A sociedade já passou por diversas formas de organização social. A cada momento o elemento central da sociedade era alterado. Na sociedade agrícola o elemento que alavancava a economia era os produtos agrícolas. Mais adiante, na sociedade industrial, as máquinas e a eletricidade eram os elementos propulsores da economia. Já no período pós Segunda- guerra Mundial, na sociedade pós-industrial, a sociedade se caracterizava pelos serviços prestados.

Atualmente, a sociedade vem se transformando com muita rapidez. Tudo isso por causa do avanço tecnológico. A sociedade passa, então, a ser impulsionada e organizada pelas informações, que, com o advento da internet, passa a ser processada e transmitida em quantidade e velocidades antes impensáveis[2].

[2] BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. Ed. – Rio de Janeiro: Forense, 2020. p. 5

Diante disso, a informação passa a ser elemento central e adjetivante na sociedade, *a sociedade da informação*.[3]

A sociedade da informação é a sociedade que tem como seu elemento principal de organização social e como vetor de desenvolvimento econômico a informação.[4]

> "A expressão "sociedade da informação" passou a ser utilizada, nos últimos anos desse século, como substituto para o conceito complexo de "sociedade pós-industrial" e como forma de transmitir o conteúdo específico do "novo paradigma técnico-econômico". A realidade que os conceitos das ciências sociais procuram expressar refere-se às transformações técnicas, organizacionais e administrativas que têm como "fator-chave" não mais os insumos baratos de energia – como na sociedade industrial – mas os insumos baratos de informação propiciados pelos avanços tecnológicos na microeletrônica e telecomunicações."[5]

É importante observar que a informação sempre teve um papel importante na sociedade. O que muda é a forma que a sociedade se estrutura centralizando a informação como modelo organizacional.

O que se faz com a informação é o ponto chave desse novo modelo de organização da sociedade. A partir do momento que a informação é processada de maneira efetiva e transformada em conhecimento, ela é tornada produtiva e ardilosa: "O que faz uma empresa ganhar dinheiro não é receber a informação em si própria. É transformar essa informação em conhecimento que

[3] BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. Ed. – Rio de Janeiro: Forense, 2020. p. 5

[4] BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. Ed. – Rio de Janeiro: Forense, 2020. p. 4

[5] WERTHEIN, Jorge. A sociedade da informação e seus desafios. <https://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf>

depois é aplicado. Falta-nos por isso introduzir a questão da transformação em conhecimento".[6]

Com essa necessidade de transformação da informação em conhecimento, os dados pessoais dos cidadãos passaram a ser um produto valioso para a economia da informação. Chega-se a dizer que os dados pessoais são o novo petróleo.[7]

Mas, onde fica o dono do dado pessoal dentro dessa economia de informação?

Nota-se que, com o surgimento do Big Data, isto é, forma de organização dos dados com a finalidade de gerar dados importantes, surgiu uma economia de vigilância, onde o dono do dado seria apenas um observador de suas informações.

No entanto, o papel de mero espectador tem ficado para trás. Em primeiro lugar, porque a dinâmica da internet, através dos algoritmos, dita para que lado a grande massa de informações está indo: no consumo, na comunicação, na política, no mercado etc., o proprietário do dado passa a ser peça central nas relações da sociedade. Conforme fala Claudio Torres[8]:

> "Novas tecnologias e aplicações, como os blogs, as ferramentas de buscas, os fóruns, as redes sociais e tantas outras aplicações on-line foram utilizadas pelos internautas para, literalmente, assumir o controle, a produção e o consumo da informação, atividades antes restritas aos grandes portais".

[6] AMARAL, João Ferreira do. Economia da Informação e do Conhecimento. Coimbra: Almedina.2009. p.116 em

[7] HUMBY, Clive. "Data is te new oil" ou Dados são o novo petróleo, em tradução livre foi uma frase utilizada pelo matemático londrino Clive Humby e pode ser encontrada em <https://en.wikipedia.org/wiki/Clive_Humby>

[8] TORRES, Cláudio. A bíblia do marketing digital: tudo o que você queria saber sobre o marketing e a publicidade na internet e não tinha a quem perguntar. São Paulo: Novatec, 2009. P 24

Além disso, o acesso à informação é tido como direito básico e fundamental dos cidadãos. Como bem asseverou o Ministro Edson Fachin, em seu voto, no julgamento da ADPF 403: "Os direitos que as pessoas têm offline devem também ser protegidos online. Direitos digitais são direitos fundamentais"[9]

Daí percebe-se que, as regulações de proteção de dados pessoais são valiosos instrumentos de defesa e proteção de direitos e liberdades fundamentais dos titulares dos dados, além de terem o potencial de alavancar avanços tecnológicos, uma vez que estimulam o desenvolvimento de soluções tecnológicas para a proteção de dados e demandam que as empresas e entidades a organizem sua informação.

2.2 Dados Pessoais e a Lei Geral de Proteção de Dados

Em muitos países já existem os regulamentos de proteção de dados pessoais. O mais conhecido é o regulamento da União Europeia, a GDPR – General Data Protection Regulation (Regulamento Geral sobre a Proteção de Dados).[10]

A edição da GDPR provocou uma corrida das empresas e dos estados- nações para uma adequação qualitativa de suas normas ao regulamento, tendo em vista que a GDPR atinge também, a depender do caso, os dados fora da sua jurisdição. Por exemplo, no caso da transferência internacional de dados pessoais, apenas os países que tenham um nível adequado de proteção de dados, poderá fazê-la.[11]

[9] FACHIN, Edson. <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf>
[10] <https://gdpr.eu/>
[11] Art. 44°, Capítulo V, do Regulamento Geral da Proteção de Dados da União Européia – GDPR. <https://gdpr.eu/>

No mesmo sentido, a LGPD demanda em seu art. 33, II, que a transferência internacional de dados só seja realizada entre países que promovam um nível adequado à lei em questão.[12]

> "Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:".

Dessa forma, fica evidente que os países que possuem uma regulamentação de dados já conseguem dirigir os desafios da transformação provocada pelo avanço da tecnologia.

No Brasil, em agosto de 2018, foi editada a lei 13.709/18, a Lei Geral de Proteção de Dados Brasileiro – LGPD, com previsão para sua entrada em vigor em agosto de 2020.

Essa lei foi bastante discutida no âmbito do legislativo e surge em um momento crucial que o mundo está passando. Das transformações tecnológicas à pandemia mundial, a LGPD proporciona o equilíbrio entre a posição do indivíduo na sociedade com o movimento econômico do Brasil, país que busca a inovação como meio de alcançar a competitividade no mercado.

Mas o que é um dado pessoal?

Nos termos do art. 5°, I,II e III da LGPD[13], um dado pessoal é "toda informação relacionada a pessoa natural identificada ou identificável". Ainda sobre a conceituação de dados pessoais, a

[12] Art. 33, Capítulo V, da Lei Geral da Proteção de Dados. <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>

[13] http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

LGPD o dividiu em duas espécies: a) dados pessoais sensíveis; e b) dados anonimizados.

Os dados pessoais sensíveis são aqueles que dizem respeito a

> "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; já o dado anonimizado é dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".[14]

Além da conceituação legal, pode-se dizer que dados pessoais são o direito individual de manter um controle daquilo que nos cerca, bem como de determinar de que forma tudo aquilo que nos diz respeito é compartilhado com outra pessoa. Como bem assevera Stéfano Rodotà: "a privacidade é o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública".[15]

A conceituação acima é importante na medida em que é de grande valia tutelar a personalidade do indivíduo contra tratamento abusivo e desleal de dados pessoais, além da preocupação com os riscos e os potenciais danos, que é o que acontece quando não se tem mais total controle sobre o que é feito com informações dos cidadãos.

Nesse sentido, seria interessante que essa nova regulação não fosse vista como mais um instrumento regulatório

[14] http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
[15] RODOTÀ, Stéfano. Data Protection as a Fundamental Right. In: In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., NOUWT S. (eds). Reinventing Data Protection? Dordrecht: Springer, 2009, p. 78.

desnecessário. É importante que empresas e órgãos saibam quais são os dados que elas possuem e o que fazer com esses dados.

Como dito mais acima, o mais importante é saber o que fazer com a informação e como transformá-la em um ativo para a sociedade.

3 DADOS PESSOAIS E CRIPTOGRAFIA

A tecnologia criptográfica nada mais é do que a codificação de uma informação sensível (dado), para que terceiros não autorizados tenham acesso a essa informação e dado. Isto é, a "criptografia é um sistema de algoritmos matemáticos que codificam dados do usuário para que só o destinatário possa ler"[16].

Dessa forma, o que se busca com essa tecnologia é preservar a integridade da informação, a confidencialidade de seu conteúdo, bem como a autenticidade das partes. [17]

A criptografia é técnica utilizada desde a antiguidade, quando a codificação do alfabeto era utilizada para antever a chegada do inimigo. Atualmente, a tecnologia criptográfica é bem mais complexa. [18]

Com o avanço da tecnologia, os dados são criptografados através de algoritmos matemáticos complexos, de difícil decodificação e que demanda computadores com tecnologia avançada, dentre outras habilidades do criptoanalista.

[16] https://canaltech.com.br/seguranca/criptografia-para-iniciantes-o-que-e-como-funciona-e-por-que-precisamos-dela-46753/

[17] ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, 2017 p.24-42

[18] ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, 2017 p.24-42

A tecnologia criptográfica é um assunto que interessa e muito ao Estado. Como uma técnica para preservar dados sensíveis, ela sempre foi utilizada para preservar privacidade e a segurança de suas próprias comunicações e dados[19].

O que não parece muito interessante para os órgãos do estado é que as grandes empresas já se utilizam da tecnologia criptográfica para resguardar os seus dados e de seus usuários. Como bem assevera Jacqueline Abreu: "Subjacente aos casos de bloqueio do WhatsApp, encontra-se o descontentamento de autoridades estatais com a impossibilidade técnica de interceptação em tempo real de conversas de suspeitos investigados, em razão da criptografia utilizada pela empresa".[20]

Em 2017, o mundo se viu às voltas de uma ciberataque denominado Wannacry. Tratava-se de uma invasão a sistemas de computadores que, explorando a vulnerabilidade do sistema Windows, bloqueava o acesso do usuário a seus arquivos, só os liberando mediante resgate. A ferramenta de invasão de sistemas de informática foi desenvolvida pela National Security Agency (NSA), uma agência de Inteligência do Estados Unidos, mas foi utilizada por hackers que tiveram acesso ao código-fonte[21].

Em outra oportunidade, um outro ciberataque mundial foi realizado. Tratava-se do DoublePulsar, uma ferramenta de ataque "porta dos fundos" (backdoors), também desenvolvida pela National Security Agency (NSA).[22] Esse ataque tinha por objetivo a

[19] ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, 2017 p.24-42

[20] ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, 2017 p.24-42

[21] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[22] https://en.wikipedia.org/wiki/DoublePulsar

obtenção de informações estratégicas e o domínio dos sistemas invadidos.

Os ataques acima não são novidades. As Crypto Wars (guerras criptográficas). Desde quando os sistemas de comunicação passaram a utilizar a tecnologia de criptografia, uma tensão opôs o Poder Público e os desenvolvedores de tecnologias.

Certo é que, o desenvolvimento de ferramentas de ataque como Wannacry e DoublePulsar por parte do Poder Público visa tão somente assegurar o bem-estar coletivo através do aprimoramento das ferramentas de investigação criminal. Como bem assevera Felipe Rocha Martins:[23]

> "Quando o Estado desenvolve ferramentas dessa natureza, não o faz com o intuito de torná-las públicas. Deve-se presumir, evidentemente, que o escopo dos desenvolvedores dos citados vetores de ataque seria o aperfeiçoamento do bem-estar coletivo pelo aprimoramento da capacidade estatal de investigar grupos criminosos, terroristas ou, mesmo, Estados rivais. Há, assim, uma aparente dicotomia, que se manifestaria na forma de um trade-off entre segurança e privacidade; esta, eventualmente, será mitigada pelo Poder Público em benefício daquela. Outrossim, o problema poderia ser reformulado da seguinte forma: quanto maior o nível de proteção à intimidade, menor seria a capacidade estatal de obter evidências no âmbito de investigações – sobretudo preventivas – que assegurem a proteção da coletividade".

Percebe-se que, para as autoridades investigativas, a mesma tecnologia que protege a privacidade do indivíduo, também abre espaço para a atuação criminosa sem o olhar estatal. É um apelo das autoridades a ampliação da capacidade investigativa em

[23] SOARES, Filipe Rocha Martins. O cobertor é muito curto: as guerras criptográficas como jogo de soma zero resultante de percepção regulatória equivocada quanto à segurança cibernética. In: FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata de (Coord.). Tecnologia jurídica & direito digital: II Congresso Internacional de Direito, Governo e Tecnologia – 2018. Belo Horizonte: Fórum, 2018. p. 285-304. ISBN 978-85-450-0584-1.

ambiente digital, como se fosse possível, atualmente, separar o mundo real do mundo digital. Seria como sobrepor a importância da segurança física, do mundo real, a segurança em meio cibernético.

3.1 O Caso WhatsApp e Tecnologia Criptográfica

No Brasil o caso mais recente e mais emblemático é o caso do bloqueio do aplicativo de mensagens WhatsApp. Desde que adotou o uso da tecnologia da criptografia, o aplicativo vem sendo alvo de decisões judiciais, tendo em vista a impossibilidade de entregar os conteúdos das mensagens trocadas por indivíduos alvo de investigações criminais e inquéritos penais, já que essas mensagens trocadas são criptografadas.

A criptografia utilizada pelo aplicativo de mensagens WhatssApp é a criptografia de ponta a ponta (end-to-end encryption), isto é, o conteúdo das mensagens só pode ser acessado pelos dois extremos da conversa[24]. Nem mesmo os aplicativos de mensagens conseguem ter acesso ao conteúdo do que foi comunicado. Trata-se de uma forma de criptografia assimétrica ne não permite que a conversa seja interceptada.

A justificativa utilizada pelo aplicativo, bem como pelos demais aplicativos de troca de mensagem é de que com a tecnologia de criptografia de ponta a ponta nem mesmo os aplicativos guardam os conteúdos das mensagens trocados por seus usuários. É como se a mensagem deixasse de existir para além do remetente e do destinatário.

Atualmente, o caso WhatsApp está sendo discutido no âmbito do Supremo Tribunal Federal, na Ação de Descumprimento de

[24] https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption

preceito Fundamental – ADPF 403, e na Ação Direta de Inconstitucionalidade – ADI.

A ADPF 403, de relatoria do Ministro Edson Fachin, discute o cabimento de ordens judiciais de bloqueio do WhatsApp com a liberdade de comunicação. Já a ADI 5527, de relatoria da Ministra Rosa Weber, discute a constitucionalidade dos incisos III e IV do art. 12 do Marco Civil do Internet (MCI), que autorizam a imposição das sanções de "suspensão temporária" e "proibição do exercício das atividades" de provedores de conexão e aplicações de internet.

Trata-se de dois casos em que se discute a quebra de sigilo de dados e comunicações em virtude do uso da criptografia pelo aplicativo.

Em audiência pública realizada no STF em junho de 2017, discutiu-se pontos cruciais a respeito das ações acima, com a finalidade de esclarecer dúvidas suscitadas pelo Tribunal[25]:

> Em que consiste a criptografia ponta a ponta (end to end) utilizada por aplicativos de troca de mensagens como o WhatsApp?
>
> Seria possível a interceptação de conversas e mensagens realizadas por meio do aplicativo WhatsApp ainda que esteja ativada a criptografia ponta a ponta (end to end)?
>
> Seria possível desabilitar a criptografia ponta a ponta (end to end) de um ou mais usuários específicos para que, dessa forma, se possa operar interceptação juridicamente legítima?
>
> Tendo em vista que a utilização do aplicativo WhatsApp não se limita a apenas uma plataforma (aparelhos celulares/smartphones), mas permite acesso e utilização também em outros meios, como, por exemplo, computadores (no caso do WhatsApp mediante o WhatsApp Web/Desktop),

[25] https://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/

> ainda que a criptografia ponta a ponta (end to end) esteja habilitada, seria possível "espelhar" as conversas travas [sic] no aplicativo para outro celular/smartphone ou computador, permitindo que se implementasse ordem judicial de interceptação em face de um usuário específico?

Percebe-se que, apesar de a discussão do Tribunal versar sobre o bloqueio ou não dos aplicativos de mensagens, é notório que o STF centralizou a discussão em torna da tecnologia de criptografia.

Os diagnósticos apresentados por especialista, dentre eles juristas, técnicos, profissionais de Tecnologia da informação, engenheiros, dentre outros, demonstra que, da forma que é formado hoje, não é possível ao WhatssApp a interceptação de mensagens.[26]

Para atender à demando do Poder Público seria necessário rever os protocolos de criptografias adotados e isso não é considerado uma ideia plausível, conforme as justificativas apresentadas a seguir:[27]

> seria ineficaz, uma vez que não impediria, na prática, que criminosos detectassem a vigilância nem tivessem acesso, por outros meios, a versões seguras de criptografia para se comunicar;
>
> fragilizaria todo a segurança do aplicativo, já que a introdução de uma forma de 'acesso excepcional' tornaria o sistema mais complexo e, por isso, mais vulnerável;
>
> traria problemas de escala, uma vez que o aplicativo teria de ser 'particularizado' para o Brasil, impondo dificuldades de gestão e execução a nível mundial;

[26] https://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/

[27] https://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/

> violaria liberdades, de programadores (de construir sistemas seguros), de usuários (de se comunicar de forma segura e privada, o que é especialmente sensível quando se pensa em ativistas de direitos humanos e profissionais como médicos, advogados e até agentes de segurança) e da empresa (de empreender e oferecer serviços seguros).

No mesmo sentido, foi ressaltada a importância de se proteger a tecnologia criptográfica, pois a proteção da criptografia, bem como dos dados pessoais, nada mais é que uma janela de oportunidades para que os órgãos públicos se modernizem e se encontrem nesse novo mundo cibernético, que hoje ocupa a vida da sociedade como um todo.[28]

Do lado do Poder Público, Ministério Público Federal, Polícia Federal, dentre outros órgãos ressaltaram a importância da criptografia, mas contra argumentaram que é papel do WhatsApp colaborar com a persecução penal quando os crimes forem realizados com a ajuda do aplicativo.[29]

Ora, atualmente não há nenhum regulamento que determine aos desenvolvedores criarem tecnologia capazes de sofrerem interceptações. Isso seria até uma forma de se causar insegurança na sociedade, tendo em vista que coloca em xeque a confiabilidade e segurança no ambiente digital, que é indispensável atualmente.

É o que o Ministro Edson Fachin deixa claro em seu voto na APF 403:[30]

> "É contraditório, portanto, que em nome da segurança pública deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado.

[28] https://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/

[29] https://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/

[30] <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf>

> Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outros áreas. Não é isso, porém, o que ocorre. O risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional".

Percebe-se que o enfraquecimento do padrão criptográfico sugerido pelos órgãos de investigação no ato da audiência, apenas tenta buscar um resulta mais rápido para a aumentar a capacidade investigativa. Essa proposta gera, indubitavelmente problemas oriundos dos ataques cibernéticos, na medida em que, o enfraquecimento da criptografia suscitada pelo Poder Público cria vulnerabilidades passiveis de ataques com alto potencial destrutivo.

Como bem salienta Felipe Rocha Martins:[31]

> "A estratégia estatal de combate, no âmbito das guerras criptográficas, é a busca de ganhos táticos em detrimento de benefícios estratégicos potencialmente advindos da compatibilização entre as duas esferas de segurança: a física e a cibernética. Configura-se, nestes termos, um jogo de soma zero. Tanto autoridades reguladoras quanto o Poder Judiciário tendem a perceber apenas benefícios de curto prazo na obtenção de dados a serem utilizados em investigações, mas ignoram os potenciais danos decorrentes da adulteração de padrões criptográficos. Custam, ademais, a perceber a dificuldade de implementação de suas decisões, nos moldes que atualmente tentam impor, em decorrência do caráter amórfico da arquitetura da internet determinada pelo código cibernético".

[31] SOARES, Filipe Rocha Martins. O cobertor é muito curto: as guerras criptográficas como jogo de soma zero resultante de percepção regulatória equivocada quanto à segurança cibernética. In: FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata de (Coord.). Tecnologia jurídica & direito digital: II Congresso Internacional de Direito, Governo e Tecnologia – 2018. Belo Horizonte: Fórum, 2018. p. 285-304. ISBN 978-85-450-0584-1.

Como já dito acima, não se deve sobrepor o direito à segurança pública em ambiente físico ao direito à segurança cibernética.

Após longa consulta aos interessados, entidades públicas e privadas, o STF iniciou o julgamento da ADI 5527 e da ADPF 403 no final de maio de 2020.

O Ministro Relator da ADPF 403 andou bem ao demonstrar questões primordiais que resguardam direitos fundamentais dos cidadãos. Salientou a importância de se debater o assunto na Suprema Corte, tendo em vista que se deve sopesar os limites das decisões judiciais que restringem o direito à privacidade: [3233]

> "A presente controvérsia emerge efetivamente a partir de decisões judiciais: trata-se, portanto, de investigar, nos termos do art. 7º, II, do Marco Civil da Internet, os limites da decisão judicial que restringe o direito à privacidade. Há, portanto, ato do poder público que, de forma geral e ampla, vulnera, ao menos no que alega o Partido, preceito fundamental".
>
> "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: 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"

Como bem assevera Edson Fachin, no artigo acima que a garantia do direito à privacidade e a liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.[34]

Como já salientado acima, a ciência jurídica deve se redescobrir com o passar do tempo. Com o avanço tecnológico

[32] <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf>
[33] <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>
[34] <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf>

essa adaptação do Direito à nova realidade em que os indivíduos vivem, é salutar. Como bem discorreu o Ministro Gilmar Mendes:[35]

> "Independente do acerto ou desacerto dessas decisões automatizadas, é inequívoco que a proteção dos valores estruturante da nossa democracia constitucional requer que o Direito atribua elementos de transparência e controle que preservem o exercício da cidadania. É por isso que, para muito além do mero debate sobre o sigilo comunicacional, este Tribunal deve reconhecer que a disciplina jurídica do processamento e da utilização da informação acaba por afetar o sistema de proteção de garantias individuais como um todo."

O que está em jogo é o alcance do direito à privacidade. Aquilo que o indivíduo consome, prática ou troca online, deve ser considerado uma garantia fundamental. Não se pode admitir excessos de qualquer lado, em especial excessos que coloquem a intimidade dos cidadãos em jogo.

De acordo com o Conselho Nacional de Justiça – CNJ, apenas no ano de 2019 foram expedidos mais de 63.303 ofícios determinando a interceptação dos sigilos de comunicação. Diante disso, o que se pode observar é uma dependência que as autoridades possuem das interceptações no bojo das investigações criminais, como se observa no quadro a seguir:[36]

---

[35] <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf>

[36] CONSELHO NACIONAL DE JUSTIÇA. Sistema Nacional de Controle de Interceptações Telefônicas. https://www.cnj.jus.br/interceptacoes_tel/relatorio_quantitativos.php. *LEGENDA. Total 1 = Quantidade de Ofícios Expedidos (inicial); Total 2 = Quantidade de Ofícios Expedidos (total em andamento); Total 3 = Quantidade de Procedimentos Criminais Instaurados (inicial); Total 4 = Quantidade de Procedimentos Criminais Instaurados (total em andamento); Total 5 = Quantidade de Telefones Monitorados (total em andamento); Total 6 = Quantidade de Telefones Monitorados - VOIP (total em andamento); Total 7 = Quantidade de Ofícios Expedidos (inicial); Total 8 = Quantidade de Ofícios Expedidos (total em andamento); Total 9 = Quantidade de Procedimentos Criminais Instaurados (inicial); Total 10 = Quantidade de Procedimentos Criminais Instaurados (total em andamento); Total 11 = Quantidade de Endereços Eletrônicos Monitorados (total em andamento)

Mês/Ano	Total 1	Total 2	Total 3	Total 4	Total 5	Total 6	Total 7	Total 8	Total 9	Total 10	Total 11
Janeiro/2019	1825	4753	575	2366	14482	1841	288	615	97	270	996
Fevereiro/2019	2664	6210	760	3119	21117	2831	437	775	145	370	1615
Março/2019	2421	5768	739	3310	19043	3270	327	625	141	488	1616
Abril/2019	2736	5676	726	2609	17901	2425	474	796	130	455	1541
Maio/2019	2631	5913	761	3313	19724	2430	466	818	172	364	1978
Junho/2019	2229	5342	677	3198	18137	2193	375	738	160	402	1395
Julho/2019	2366	5658	730	3260	20323	2060	354	679	144	353	1351
Agosto/2019	2735	5699	713	3115	18005	2136	379	783	142	478	1158
Setembro/2019	2183	5182	653	3038	16517	2176	361	683	142	373	1132
Outubro/2019	1962	4961	581	2779	17063	2208	253	614	125	350	1441
Novembro/2019	1809	4535	511	2449	15520	1922	240	565	96	416	1037
Dezembro/2019	1431	3606	393	1645	10686	1572	218	507	78	277	811
Total	**26992**	**63303**	**7819**	**34201**	**208518**	**27064**	**4172**	**8198**	**1572**	**4596**	**16071**

A liberdade de expressão, seja ela exercida em blogs, redes sociais ou conversas privadas por meio de aplicativos de mensagens, deve ser vista e reconhecida como liberdade de expressão e comunicação, prevista no art. 5°/CF. Até mesmo porque o fluxo de informações é composto de dados de propriedade dos usuários.

Seguindo a mesma linha do Ministro Edson Fachin, a Ministra Rosa Weber, em seu voto na ADI 5527, ressaltou a importância da criptografia para se resguardar os direitos fundamentais da privacidade e do sigilo nas comunicações.[37]

> "Trata-se, pois, de tecnologia que atua no sentido da realização material da garantia de preservação do sigilo das comunicações consagrada no art. 5º, XII, da CF. Entendimento diverso significaria submeter a regra, que é a proteção do sigilo das comunicações, à exceção, que é o acesso do

[37] <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf>

> Estado ao conteúdo da comunicação privada no curso da persecução criminal."

A criptografia é artificio de grande utilidade para o compartilhamento de opiniões. Protege-se com ela direitos necessários para a vida na sociedade. A justiça não deve demandar em suas decisões medidas que são impossíveis de serem adotadas pela parte. Caso conseguisse cumprir a decisão de interceptar as conversar de usuários, estaria o aplicativo insurgindo-se contra garantias constitucionais dos indivíduos.

4 CONCLUSÃO

A proteção dos dados pessoais e a tecnologia nunca tiveram um papel tão importante na sociedade como atualmente.

Em um momento em que a proteção aos direitos fundamentais dos cidadãos está na pauta dos maiores tribunais do país, faz-se necessário discutir amplamente os limites da atuação estatal e os limites do uso da tecnologia diante desse movimento ligeiro de inovação tecnológica.

Apesar da LGPD ainda não ter entrado em vigor e não tratar diretamente da segurança pública, a sua citação é importante, na medida em que conceitua o que é dados pessoal, bem como demonstra a corrida para se regular o uso do dados pessoais no Brasil, bem como o interesse de diversos setores da sociedade na busca por uma maior segurança da informação.

No entanto, vê-se que mesmo com a edição da LGPD, ainda não se tomaram medidas concretas para a criação da Autoridade Nacional de Proteção de Dados – ANPD.

A criação da autoridade se faz necessária, pois a judicialização das questões que envolvem direito à proteção de dados dos indivíduos deve continuar em grande medida.

O sigilo de dados e das comunicações é garantia constitucional e, com a sua devida importância, deve ser respeitada.

As ações propostas no Supremo Tribunal Federal, ADPF 403 e ADI 5527 são demonstrações da tensão que existe entre o Poder Público e as empresas de tecnologia e de comunicação. É um verdadeiro cabo de guerra em que ninguém sai ganhando. O cidadão não pode ser penalizado tendo a sua vida privada colocada em situação de vulnerabilidade, para que um grupo de cidadão criminosos seja investigado.

Não se pretende aqui diminuir a importância do combate ao crime. O que se pretende é dar a chance ao Poder Público de refletir e buscar outras formar de conduzir a persecução penal, sem que seja necessário enfraquecer uma tecnologia que tanto serve para a proteção de direitos e garantias fundamentais dos indivíduos. Olhando por outro lado, cabe às empresas de tecnologia atuarem em parceria ou, até mesmo, pensarem em desenvolver mecanismos de coibição da prática de crimes.

Nota-se que, atualmente, existem outras tecnologias que poderiam ser utilizadas para o combate ao crime virtual: infiltrações, metadados, dados em nuvens são opções de que o Poder Público pode se valer para alcançar os dados desejados em suas investigações.

A guerras criptográfica desenvolvem um papel importante no mundo. Para esse trabalho importa a proteção da coletividade e a proteção da privacidade e intimidade dos indivíduos. No entanto, as Cryptowars demonstram a tentativa de conciliação entre o mundo real e o mundo digital.

Há que se buscar instrumentos de compatibilização entre o mundo físico e o mundo cibernético, sem, contudo, inviabilizarem o poder de segurança do estado e nem ferir direito e garantias constitucionais dos indivíduos. Enfraquecer a tecnologia criptográfica em busca de se resguardar a segurança pública significa deixar de promover uma internet segura, o que é direito de todos.

Não se buscou com esse trabalho esgotar qualquer discussão acerca da postura do estado em sua atuação no combate ao crime, e nem opor o Estado à tecnologia. Buscou-se mostrar que, assim como os avanços tecnológicos, o Estado tem o dever de buscar meios de inovação e atualização do seu trabalho. Trata-se de uma tentativa de conciliação de dois mundos: o mundo real e o mundo cibernético.

REFERÊNCIAS

ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, 2017 p.24-42

AMARAL, João Ferreira do. Economia da Informação e do Conhecimento. Coimbra: Almedina.2009. p.116 em

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. Ed. – Rio de Janeiro: Forense, 2020. p. 5

SOARES, Filipe Rocha Martins. O cobertor é muito curto: as guerras criptográficas como jogo de soma zero resultante de percepção regulatória equivocada quanto à segurança cibernética. In: FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata de (Coord.). Tecnologia jurídica & direito digital: II Congresso Internacional de Direito, Governo e Tecnologia – 2018. Belo Horizonte: Fórum, 2018. p. 285-304. ISBN 978-85-450-0584-1.

TORRES, Cláudio. A bíblia do marketing digital: tudo o que você queria saber sobre o marketing e a publicidade na internet e não tinha a quem perguntar. São Paulo: Novatec, 2009. P 24

DOCUMENTO ELETRÔNICOS

CONSELHO NACIONAL DE JUSTIÇA. Sistema Nacional de Controle de Interceptações Telefônicas. Disponível em: <https://www.cnj.jus.br/interceptacoes_tel/relatorio_quantitativos.php>

BRASIL. CONSTITUIÇÃO FEDERAL DE 1988. Disponível em: <https://www.senado.leg.br/atividade/const/con1988/con1988_15.12.2016/art_6_.asp >

BRASIL. Bloqueios do WhatsApp. Disponível em: <https://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/>

BRASIL. Disponível em: https://canaltech.com.br/seguranca/criptografia-para-iniciantes-o-que-e-como-funciona-e-por-que-precisamos-dela-46753/

BRASIL. LEI DO MARCO GERAL DA INTERNET. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>

BRASIL. LEI GERAL DA PROTEÇÃO DE DADOS. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>

BRASIL. FACHIN, Edson. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf>

BRASIL.WEBWER, ROSA. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf>

DOUBLEPULSAR. Disponível em: <https://en.wikipedia.org/wiki/DoublePulsar>

<https://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf>

UNIÃO EUROPÉIA. GENERAL DATA PROTECTION REGULATION. Disponível em: <https://gdpr.eu/>

WANNACRY. Disponível em: <https://en.wikipedia.org/wiki/WannaCry_ransomware_attack>

WERTHEIN, Jorge. A sociedade da informação e seus desafios. Disponível em: <https://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf>

CRIMES CIBERNÉTICOS: COMBATE À PORNOGRAFIA INFANTO-JUVENIL E À

Beatriz Cadore Martins Silva[1]

RESUMO

O presente artigo pretende demonstrar que nos últimos anos a evolução da Internet não só favoreceu de forma exponencial os padrões de vida mundial, como também fez surgir uma problemática de grande repercussão: sua utilização para cometimentos de crimes. Através de revisão bibliográfica e de material publicado, é discutido os entraves de seu processo, bem como os principais aspectos dos crimes cibernéticos, com enfoque na dificuldade de estabelecer um escopo preciso dos crimes de pedofilia e de pornografia infantojuvenil, que aumentaram com o estabelecimento da internet.

Palavras-chave: Crimes cibernéticos. Pornografia infanto-juvenil. Pedofilia.

ABSTRACT

This article intends to demonstrate that in recent years the evolution of the Internet has not only exponentially favored the living standards of the world, but has also raised a problem of great repercussion: its use for crimes. Through a bibliographic review and published material, the obstacles to its process are discussed, as well as the main aspects of cyber crimes, focusing on the difficulty of establishing a precise scope of crimes of pedophilia

[1] Advogada. Aluna do curso de pós-graduação *lato sensu* em Direito do Centro Universitário de Brasília – UniCEUB/ICPD. E-mail: beatrizcmsilva@gmail.com.

and child pornography, which has increased with the establishment of the internet.

Keywords: Cybercrimes. Child pornography. Pedophilia.

1 INTRODUÇÃO

Com o avanço tecnológico a que assistimos nos últimos anos, é evidente o papel que a Internet, enquanto meio de comunicação e informação, ocupa em nosso cotidiano. O surgimento das redes sociais atrelado aos mais variados serviços disponíveis em benefício da comunidade internacional, com certeza se insere no conceito de sociedade moderna.

O número total de usuários da internet no Brasil estimado em 2018, segundo pesquisa do Instituto Brasileiro de Geografia e Estatística, foi de 120,7 milhões, mais de 70% da população. Em relação aos jovens entre 10 e 15 anos, 89% tiveram acesso à rede.

Contudo, com o advento da sociedade digital, não só os aspectos positivos da rede se difundem, os criminosos encontraram um ambiente poderoso para a prática delitiva. Os crimes tomaram grandes proporções e apresentam desafios em seu combate, destacando a dificuldade que se tem na identificação de seus agentes.

Atrelado a isso, ainda temos a vulnerabilidade das crianças no mundo digital, que pelo uso desordenado da internet sem vigilância de seus responsáveis, fornecem informações pessoais sem temer o seu destino e, acabam por se tornar vítimas de crimes cibernéticos, destacando neste trabalho a prática dos crimes de pedofilia e de pornografia infantojuvenil.

Assim, o presente artigo utilizou como metodologia uma pesquisa bibliográfica e de material publicado relacionados a

temática escolhida: utilização da rede mundial de computadores para cometimento dos crimes de pedofilia e de pornografia infantil.

O presente trabalho foi então estruturado nas seguintes seções: na seção dois apresentam-se um histórico da globalização e da internet e sua relação com os crimes digitais; a seção três proporciona uma análise sobre os crimes cibernéticos, seu conceito e sua classificação, bem como a importância da Convenção de Budapeste na tentativa de harmonizar legislações penal e processual penal que abordam o assunto; por fim, na seção quatro apresenta-se um panorama da dificuldade de identificação dos agentes dos crimes de pedofilia e de pornografia infantil na internet.

2 A GLOBALIZAÇÃO E A INTERNET

Depreende-se por globalização as mudanças ocorridas na última década do século XX, que originaram um mundo fundamentado em novas estruturas sociais, culturais, tecnológicas e econômicas. Ou seja, trata-se de um processo histórico complexo que tem seu núcleo vinculado à crescente intensificação das relações sociais em escala mundial, influenciados especialmente no desenvolvimento dos sistemas de comunicação criados no final da década de 60[2].

A globalização tornou-se responsável pela universalização de muitas áreas após a Segunda Guerra Mundial, bem como pela integração entre os Estados Soberanos, mediante eficientes tecnologias de comunicação, o que contribuiu para o desenvolvimento de atividades econômicas lícitas e ilícitas, pois os

[2] KESIKOWSKI, Sabrina Cunha; WINTER, Luis Alexandre Carta; GOMES, Eduardo Biacchi. *Atuação do Grupo Mercado Comum frente à criminalidade organizada transnacional.* Revista de Direito Internacional, v. 15, n. 2, p. 353-369, 2018. Acesso em: 07/05/2020.

mesmos mecanismos utilizados pelo mercado capitalista legítimo também favorecem os grupos criminosos em todo o globo[3].

Os meios virtuais – como sítios de busca, dos provedores de acesso e de conteúdo, de redes sociais – são favoráveis para condutas perniciosas de criminosos de todos os matizes, podendo essas condutas configurar em crimes como calúnia, ameaça, pornografia infantil, falsa identidade, pedofilia[4].

É evidente, portanto, a vulnerabilidade das pessoas ao terem seus dados circulando pela grande rede de computadores, pois os crimes que anteriormente eram praticados apenas no plano nacional agora são cometidos internacionalmente[5].

Ocorre que a utilização da internet não se limita aos adultos. É cada vez mais frequente o uso da rede por crianças através de celulares, tablets e computadores. Os jovens usuários fornecem informações pessoais na rede sem temer o seu destino e, acabam por se tornar vítimas de crimes digitais. As crianças e adolescentes se expõe a situações de alto risco, consequência do uso desordenado da internet sem vigilância de seus responsáveis. Ainda mais preocupante, são os crimes informáticos praticados por adultos que têm como vítimas as crianças[6].

---

[3] KESIKOWSKI, Sabrina Cunha; WINTER, Luis Alexandre Carta; GOMES, Eduardo Biacchi. *Atuação do Grupo Mercado Comum frente à criminalidade organizada transnacional.* Revista de Direito Internacional, v. 15, n. 2, p. 353-369, 2018. Acesso em: 07/05/2020.

[4] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 158. Acesso em: 08/05/ 2020.

[5] KESIKOWSKI, Sabrina Cunha; WINTER, Luis Alexandre Carta; GOMES, Eduardo Biacchi. *Atuação do Grupo Mercado Comum frente à criminalidade organizada transnacional.* Revista de Direito Internacional, v. 15, n. 2, p. 353-369, 2018. Acesso em: 07/05/2020.

[6] EUFRASIO, Emília Teixeira Lima. *O Cibercrime e a violação dos Direitos Fundamentais de natureza pessoal dos menores*. Tese apresentada no Programa de Mestrado em Direito de Universidade Fernando Pessoa, sob a orientação do Professor João Casqueira. Porto, 2015, p. 5. Acesso em: 08/05/2020.

De acordo com pesquisa efetuada pelo Instituto Brasileiro de Geografia e Estatística[7] (IBGE), no ano de 2018 (última atualização), o Brasil possuía mais de 120,7 milhões de internautas, o que representava mais de 70% da população. Verificou-se, ainda, que 89% das crianças entre 10 e 15 anos tiveram acesso à internet.

É notório o elevado número de acesso à rede mundial de computadores, uma vez que a mesma beneficia a comunicação entre as pessoas de forma rápida e eficiente. Contudo, deve-se ter conhecimento do ônus que pode ser gerado pela falta de conhecimento e até mesmo de cuidados básicos no acesso, ocasionando prejuízos aos mais variados bens jurídicos tutelados[8].

Contudo, o Direito Penal e suas legislações criminais especiais não conseguem prever as evoluções tecnológicas, fato que ocasiona problemas, pois a ausência de norma incriminadora para certas condutas praticadas no mundo virtual impede a aplicação de uma sanção adequada para seus agentes. Tem-se, assim, uma fragilidade do direito em virtude dessa realidade social[9].

Cabe pontuar, que a globalização trouxe consigo novas formas de interação virtual, que influencia positivamente diversos ramos, como econômicos, industriais, entre outros. No entanto, somado a estas melhorias há a necessidade do aprimoramento dos

[7] Tutorial Teleco. Internet no Brasil – Perfil dos usuários. Disponível em: < https://www.teleco.com.br/internet_usu.asp>. Acesso em 07/05/2020.

[8] MACHADO, Thiago José Ximenes. *Cibercrime e o crime no mundo informático*. Tese apresentada no Programa de Mestrado em Criminologia da Universidade Fernando Pessoa, sob a orientação da Professora Rita Rola. Porto, 2017. Porto, 2017, p. 6. Acesso em: 07/05/2020.

[9] MACHADO, Thiago José Ximenes. *Cibercrime e o crime no mundo informático*. Tese apresentada no Programa de Mestrado em Criminologia da Universidade Fernando Pessoa, sob a orientação da Professora Rita Rola. Porto, 2017, p. 7. Acesso em: 07/05/2020.

mecanismos de combate à criminalidade transnacional, bem como o dever de repensar a Ciência Criminal, com o intuito de combater as novas modalidades criminosas[10].

2.1 Histórico da internet

É certo que a Internet, enquanto meio de comunicação e informação, ocupa em nosso cotidiano um papel de extrema importância e destaque. O grande volume de informação em benefício da comunidade internacional atrelado aos mais variados serviços disponíveis na rede de computadores com certeza é elemento fundamental no conceito de sociedade moderna[11].

Quanto às origens da Internet, é evidente a contribuição das guerras para toda inovação tecnológica, pela influência no desenvolvimento e bem-estar dos cidadãos. Durante a Segunda Guerra Mundial, houve a necessidade da criação de meios eficazes para calcular a tabela de artilharia, o que levou ao surgimento do primeiro computador eletroeletrônico, o *Automatic Sequence Controlled Calculator* (ASCC)[12].

Na década de 60, a rede antecessora à Internet, a *Advanced Research Projects Agency Network* (ARPANET), nasceu de um projeto de governo mantido pelo Departamento de Defesa Norte-Americano, com o objetivo de estimular a pesquisa em

[10] MACHADO, Thiago José Ximenes. *Cibercrime e o crime no mundo informático*. Tese apresentada no Programa de Mestrado em Criminologia da Universidade Fernando Pessoa, sob a orientação da Professora Rita Rola. Porto, 2017, p. 7. Acesso em: 07/05/2020.

[11] SILVA, João Miguel Almeida da. *Cibercrime: O Crime de Pornografia Infantil na Internet.* Tese apresentada no Programa de Mestrado em Direito da Universidade de Coimbra, sob a orientação da Prof. Ana Rita da Silva Samelo Alfaiate. Coimbra: Universidades de Coimbra, 2016. Acesso em: 11/05/2020.

[12] MAZONI, Ana Carolina. *Crimes na Internet e a Convenção de Budapeste*. Tese apresentada no Programa de Bacharelado em Direito do Centro Universitário de Brasília (UniCEUB), sob a orientação do Professor George Leite. Brasília: UniCEUB, 2009, p. 8. Acesso em: 8/05/2020.

computação interativa através de algumas centenas de computadores interconectados[13]. Outro benefício dessa rede era a otimização do tempo de uso desses equipamentos. Este sistema era formado por um computador central que processava e armazenava todas as informações compartilhadas com vários terminais, que eram usados por alunos do Departamento de Computação do *Massachusetts Institute of Technology* (MIT)[14].

Na década de 70, outras iniciativas similares também existiam, que utilizavam protocolos diferentes, como as redes CYCLADES (França), Mark I (Reino Unido), Telenet e Merit Network (EUA). O princípio em comum entre estes sistemas era a contratação de pacotes, método de transmissão de dados em rede sem a necessidade de canais específicos para cada conexão[15].

Na década de 80, em meio à evolução da Internet, e diante da necessidade de um novo modelo de gerenciamento para esta rede, o governo norte americano financiou uma força-tarefa formada por 21 pesquisadores denominada de *Internet Engineering Task Force* (IETF). O intuito deste trabalho era auxiliar com o desenvolvimento da rede mediante um modelo de gestão cooperativa, fundada em consenso, envolvendo uma variedade de setores e indivíduos. No entanto, na década de 90, houve a associação do IETF com a empresa privada *Internet Society,* com o objetivo de garantir que nenhum governo tivesse o domínio das

[13] MINISTÉRIO PÚBLICO FEDERAL. *Roteiro de Atuação Crimes Cibernéticos*. 2.ª Câmara de Coordenação e Revisão da Procuradoria-Geral da República 3.ª Edição. Brasília, 2016, p. 32. Acesso em: 8/05/2020.

[14] CORREA, Fabiano Simões. *Um estudo qualitativo sobre as representações utilizadas por professores e alunos para significar o uso da internet.* Tese apresentada no Programa de Pós-Graduação em Psicologia da Universidade de São Paulo [USP], sob a orientação do Prof. Sergio Kodato. Ribeirão Preto: USP, 2013, p. 18.

[15] MINISTÉRIO PÚBLICO FEDERAL. *Roteiro de Atuação Crimes Cibernéticos*. 2.ª Câmara de Coordenação e Revisão da Procuradoria-Geral da República 3.ª Edição. Brasília, 2016, p. 89. Acesso em: 08/05/ 2020.

decisões, tornando-se, assim, uma organização independente do governo dos Estados Unidos[16].

Nos dias atuais, há uma variedade de formas de se conectar à internet. Entre os meios de acesso mais utilizados destacam-se os aparelhos celulares e o uso da estrutura de telefonia fixa. Em áreas mais distantes dos centros urbanos, a conexão via satélite é a opção mais popular. Redes acadêmicas e corporativas utilizam tecnologias mais robustas para conexão, podendo citar as estruturas de fibra ótica. Ou seja, independente do meio de conexão escolhido pelo internauta, esse estará envolvido no mesmo conglomerado de redes, que é a Internet[17].

No início, não havia razões para se preocupar com questões mais críticas de segurança da rede. Com o aumento dos relacionamentos entre pessoas de diferentes países e a importância que a Internet começou a exercer nas tarefas rotineiras e por vezes criticadas da vida moderna, que dependem hoje do bom funcionamento da rede, surgiu uma problemática de grande repercussão, a utilização da Internet para o cometimentos de crimes, os chamados "ciberataques'[18].

Os problemas envolvendo a utilização equivocada da Internet surgiram quando a população em geral passou a ter acesso livre à

[16] MINISTÉRIO PÚBLICO FEDERAL. *Roteiro de Atuação Crimes Cibernéticos*. 2.ª Câmara de Coordenação e Revisão da Procuradoria-Geral da República 3.ª Ediçã0. Brasília, 2016, p. 89. Acesso em: 8/05/2020.

[17] MINISTÉRIO PÚBLICO FEDERAL. *Roteiro de Atuação Crimes Cibernéticos*. 2.ª Câmara de Coordenação e Revisão da Procuradoria-Geral da República. 3.ª Ediçã0. Brasília, 2016, ps. 32-89. Acesso em: 08/05/ 2020.

[18] MINISTÉRIO PÚBLICO FEDERAL. *Roteiro de Atuação Crimes Cibernéticos*. 2.ª Câmara de Coordenação e Revisão da Procuradoria-Geral da República. 3.ª Edição. Brasília, 2016, p. 74. Acesso em: 08/05/2020

rede, saindo do âmbito científico e alcançando o âmbito do homem comum[19].

O Brasil está entre os quatro maiores polos de divulgação de pornografia infantil do mundo, concorrendo com os Estados Unidos, Rússia e a Coreia do Sul. Nessa realidade assustadora, a internet é um facilitador entre os criminosos, possibilitando as trocas de arquivos contendo informações, fotos e vídeos[20].

Assim, é possível perceber o constante perigo que as crianças sofrem nesse universo obscuro, pois nele os mais variados delitos são praticados, podendo acarretar danos psíquicos e físicos com consequências desastrosas como o estupro e até a morte[21].

3 CRIMES CIBERNÉTICOS

A sociedade subestima os perigos da conectividade. Até mesmo nas sociedades tradicionalmente fechadas, onde a desconfiança em relação a estranhos é diariamente advertida as crianças, como a norte-americana, não tomam os mesmos cuidados no ambiente digital[22].

O desenvolvimento da tecnologia de informação e o grande número de usuário novos da Internet, transformam as relações

[19] MAZONI, Ana Carolina. *Crimes na Internet e a Convenção de Budapeste*. Tese apresentada no Programa de Bacharelado em Direito do Centro Universitário de Brasília (UniCEUB), sob a orientação do Professor George Leite. Brasília: UniCEUB, 2009, p. 11. Acesso em: 8/05/2020.

[20] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernéticos*. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 252. Acesso em: 11/05/ 2020.

[21] MACHADO, Thiago José Ximenes. Cibercrime e o crime no mundo informático. Tese apresentada no Programa de Mestrado em Criminologia da Universidade Fernando Pessoa, sob a orientação da Professora Rita Rola. Porto, 2017, p. 12. Acesso em: 07/05/2020.

[22] BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. Cibercrimes e seus Reflexos no Direito Brasileiro. São Paulo: JusPodivm, 2020, p. 49. Acesso em:11/05/2020.

sociais e comerciais, que passam a ocorrer em tempo real, encurtando as distancias e rompendo as barreiras de espaço e tempo[23].

A Internet não possui fronteira, foi criada para ser, a princípio, acessada de qualquer parte do mundo. Ou seja, a realidade virtual não respeita as barreiras de delimitação física dos territórios dos Estados[24]. Acerca desse perigo, assevera Brtiz[25]:

> No entanto, o advento da tecnologia reduziu as barreiras tradicionais e, em verdade, serviu como um convite informal a visitantes desconhecidos. Muitos perceberam tarde demais os perigos de sua desatenção e se tornaram vítimas de furto, da perda de dados privados e similares. Outros permanecem ignorantes de sua vulnerabilidade, prestes a sofrerem as consequências de sua postura.

O real despreparo dos internautas em relação aos aspectos de Segurança de Informação ao se conectar à rede mundial de computadores no conforto de casa, tem facilitado de forma crescente o cibercrime[26].

3.1 Conceito

A tentativa de encontrar uma nomenclatura que englobe os delitos possíveis de ser cometidos na *web* é uma questão complexa. Com as constantes inovações tecnológica, alguns termos ou expressões podem soar estranhos em um primeiro

[23] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 32. Acesso em: 8/05/2020.

[24] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 32. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes. Acesso em: 8/05/2020.

[25] BRITZ, Marjie T. *Computer forensics and cybercrime: an introduction*. New Jersey: Pretice Hall, 2009, p. 4.

[26] BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. *Cibercrimes e seus Reflexos no Direito Brasileiro*. São Paulo: JusPodivm, 2020, p. 50. Acesso em: 11/05/2020.

momento. Acredita-se que isso ocorre por dois motivos: (a) a intensa evolução tecnológica influencia no surgimento de novos mecanismos e aparelhos, interferindo no vocabulário; (b) os termos são criados na língua inglesa e, depois traduzidos ao português, havendo, assim, a presença de neologismos[27].

Verifica-se, pois, algumas denominações, dentre as quais "crimes cibernéticos", "crimes eletrônicos", "crimes informáticos" ou "crimes digitais"[28].

Apesar de não existir um consenso tanto na doutrina, quanto na jurisprudência dos tribunais superiores, o Instituto Brasileiro de Direito Eletrônico[29] tem entendimento no sentido de que a melhor nomenclatura seria "crime eletrônico"[30].

Aduz Rossini[31], estudioso do tema, que a melhor nomeação é aquela que contém o termo "informático" em sua composição:

> Ouso denominá-los "delitos informáticos", pois dessa singela maneira abarcam-se não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa

[27] CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2017.

[28] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 201. Acesso em: 11/05/2020.

[29] O Instituto Brasileiro de Direito Eletrônico foi fundado em 2002, com o intuito de aprimorar o estudo do Direito Eletrônico. É uma importante rede de profissionais, cujo intuito é desenvolver a interdisciplinaridade no que tange aos temas sobre internet e mundo virtual. Entre seus trabalhos, muitas vezes desenvolvidos com parceiros, como a ONG Marias da Internet, está uma capacitação de profissionais para serem referência no atendimento às vítimas da chamada "pornografia de vingança. MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 201. Acesso em: 11/05/2020

[30] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 201. Acesso em: 11/05/2020

[31] ROSSINI, Augusto Eduardo de Souza. *Brevissímas considerações sobre delitos informáticos.* Caderno Jurídico, Ano 2, n. 4, 2002, p. 133. Disponível em: < http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Cadernos_Tematicos/direito_e_internet.pdf>. Acesso em: 11/05/2020.

> denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível "conexão" à Rede Mundial de Computadores.

Por sua vez, Sandra Govêa vale-se do termo "crimes por meio da informática", salientando que os computadores não são os únicos instrumentos capazes se serem utilizados no cometimento dos delitos[32].

Todavia, nenhum dos termos é perfeito, uma vez que todos sofrem uma ou mais deficiências, não alcançando com precisão todo o sentido dessa recente categoria de delitos. As expressões que contêm o vocábulo "computador" podem não albergar as infrações cometidas contra as redes de dados; o termo "cibercrime" pode ter enfoque único a internet; "crimes de alta-tecnologia" podem gerar referência apenas aos delitos envolvendo avançadas searas da tecnologia, como a bioengenharia e a nanotecnologia[33].

Segundo interpretação majoritária da doutrina jurídica penal moderna, delitos informáticos seriam gênero, e o delito cibernético – como enuncia o aludido autor, este se refere tão somente aos delitos ocorridos especificamente no âmbito virtual, cabendo também a expressão "delito telemático" – é espécie[34].

Tal dificuldade não ocorre apenas no Brasil, mas também no exterior, que tende a acatar a nomenclatura "delito informático" como a mais adequada. Os ordenamentos jurídicos internacionais também utilizam o mesmo termo para mencionar os problemas de

[32] CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2017.

[33] BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. *Cibercrimes e seus Reflexos no Direito Brasileiro*. São Paulo: JusPodivm, 2020, p. 52. Acesso em: 11/05/ 2020.

[34] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernéticos*. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 202. Acesso em: 11/05/ 2020

ordem civil e criminal que permeiam a via na rede. Nos países francófonos é denominado de *Droit de Línformatique*; naqueles de língua espanhola, de *Derecho de Informatica*; para os italianos é conhecido como *Diritto dell'Informatica*, e para os ingleses e norte-americanos, *Computer Law* ou *Cyber Law*[35].

Nas palavras de Mário Antônio Lobato de Paiva[36], o "direito informático" nada mais é senão o:

> [...] conjunto de normas e instituições jurídicas que pretendem regular aquele uso dos sistemas de computador – como meio e como fim – que podem incidir nos bens jurídicos dos membros da sociedade; as relações derivadas da criação, uso modificação, alteração e reprodução do software; o comercio eletrônico, e as relações humanas realizadas de maneira sui generis nas redes, em redes ou via internet.

Observa-se, ainda, a existência de duas correntes doutrinárias no que diz respeito ao reconhecimento do Direito Informático como ramo jurídico autônomo. Inicialmente, os partidários do tradicionalismo negam sua autonomia, ao passo que outros da mesma corrente consideram que as novas práticas – de caráter penal, consumerista, civil, dentre outros – no meio virtual representam um meio e, por conseguinte, são meros reflexos de condutas antes reguladas[37].

Para a segunda corrente, é indiscutível a necessidade de organizar as atividades informáticas legislativamente. Ademais, asseveram que o Direito Penal do século XIX restringe-se, em sua

[35] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 202. Acesso em :11/05/ 2020

[36] PAIVA, Mário Antônio Lobato de. Os institutos do Direito Informático. Âmbito Jurídico, Rio Grande, VI, n. 14, 2003. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-14/os-institutos-do-direito-informatico/>. Acesso em: 11/05/2020.

[37] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 203. Acesso em: 11/05/2020

maioria, aos bens jurídicos positivados na primeira e na segunda dimensão dos Direito Fundamentais[38].

3.2 Classificação

Cumpre assinalar que são essencialmente duas as categorias empregadas para categorizar os chamados crimes cibernéticos: a dos crimes informáticos próprios (ou puros) e a dos crimes informáticos impróprios (ou mistos), como bem esclarece Marcelo Crespo[39]:

> 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 (h*acking*), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas; e Crimes digitais impróprios ou mistos (conduta 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 de pornografia infantil, o estelionato e até mesmo o homicídio.

Portanto, os crimes informáticos são tantos os crimes tradicionais, já previstos na legislação brasileira, contra os bens jurídicos, praticados com auxílio da rede mundial de

[38] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 203. Acesso em: 11/05/2020

[39] CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais: do que estamos falando?* Disponível em: < https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/>. Acesso em: 11/05/2020.

computadores, além das condutas ilícitas passíveis de penas contra os sistemas informatizados e os dados[40].

Nota-se também que a velocidade na mudança dos hábitos da sociedade, em função dos usos de novas tecnologias, traz consigo um grande desafio na adaptação e definição de regras de boas condutas, as quais muitas vezes são utilizadas de forma indevida e exploradas por mentes criminosas. Do mesmo modo, a rede mundial de computadores possibilitou novas maneiras de interação social, as quais facilitaram a aplicação de golpes e o cometimento de crimes[41].

Mesmo que a utilização de computadores não seja algo novo na sociedade, o fato de a legislação brasileira não estar pronta, precisa ser revista, com o objetivo de possibilitar a adequada tipificação das diversas modalidades de crimes eletrônicos[42].

3.3 Jurisdição e os Cibercrimes: Convenção de Budapeste

A Convenção de Budapeste foi o primeiro tratado internacional sobre os cibercrimes, firmado no âmbito do Conselho da Europa, na tentativa de harmonizar legislações penal e processual penal, a fim de permitir a cooperação entre nações para obtenção de provas digitais. A *Convention on Cybercrime*, foi assinada no dia 23 de novembro de 2001, na Hungria, e aberta

[40] CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais: do que estamos falando?* Disponível em: < https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/>. Acesso em: 11/05/2020.

[41] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 16. Acesso em: 11/05/2020.

[42] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 17. Acesso em: 11/05/2020.

para adesão e ratificação dos demais Estados, tendo sido homologada por 52 signatários[43].

Nela, os Estados Partes comprometem-se a adaptar suas legislações aos termos definidos no presente instrumento jurídico internacional, especialmente no âmbito penal, além de concordarem quanto à necessidade de cooperação ao combate aos crimes cibernéticos[44].

O Brasil não é signatário da referida convenção, mas pelo fato de ser o único tratado que aborda sobre crimes na rede mundial de computadores, acaba sendo uma diretriz a ser seguida como modelo e parâmetro para as demais legislações45.

No tocante à preservação e obtenção das provas no meio informático, a Convenção de Budapeste orienta que haja preservação de dados, quando solicitado, pelo prazo de 90 dias, prorrogável por igual período. Ainda determina quanto ao auxílio mútuo para fornecimento de dados de tráfego, bem como a interceptação de conteúdo46.

Em relação ao acesso a dados armazenados fora do território de cada Estado signatário, a disposição no art. 32[47] é superficial:

---

[43] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 35. Acesso em: 11/05/2020.

[44] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 168. Acesso em: 11/05/020.

[45] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 35. Acesso em: 11/05/2020.

[46] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 35. Acesso em: 11/05/2020.

[47] CONVENÇÃO SOBRE O CIBERCRIME. Budapeste, 2011. Disponível em: < http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d76574339305a58683062334d76634842794d544d794c5668664d53356b62324d3d&fich=ppr132-X_1.doc&Inline=true>. Acesso em: 11/05/2020.

> Artigo 32.º – Acesso transfronteiriço a dados armazenados num computador, mediante consentimento ou quando se trate de dados acessíveis ao público
>
> Uma Parte pode, sem autorização de uma outra Parte:
>
> a) aceder a dados informáticos acessíveis ao público (fonte aberta), independentemente da sua localização geográfica;
>
> b) através de um sistema informático situado no seu território, aceder a dados informáticos no território de uma outra Parte, ou recebê-los, se obtiver o consentimento legal e voluntário da pessoa com legitimidade para lhe divulgar os dados através desse sistema informático.

Dessa forma, há a possibilidade de aquisição de dados informáticos armazenados fora do território nacional de cada Estado Parte, sendo válidos no âmbito processual, quando tais informações são públicas, ou seja, podem livremente ser acessadas de qualquer local ou quando se tem a autorização voluntária de quem estaria legalmente autorizado a fornecê-las[48].

Contudo, há casos em que as Cortes americanas, europeias e também brasileiras decidido que têm respaldado a necessidade de obtenção de provas eletrônicas, que não seriam alcançadas pela jurisdição do Estado onde a investigação se desenvolve[49].

4 COMBATE À PORNOGRAFIA INFANTOJUVENIL E À PEDOFILIA NA INTERNET

Normalmente as forças da lei utilizam programas de investigação em servidores que fiscalizam e informam cada vez que um arquivo com conteúdo suspeito é encaminhado ou

[48] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 36. Acesso em: 11/05/2020.

[49] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 36. Acesso em: 11/05/2020.

armazenado. Esses programas têm como fundamento as bibliotecas de *hash*[50] e apresentam, como qualquer outro sistema, inefetividade – quando novos arquivos não são identificados, por não existir *hash* catalogado na biblioteca[51].

É necessário, portanto, que os órgãos de investigação busquem meios viáveis e de rápida implementação, em termos de legislação nacional e cooperação internacional, por meio de ferramentas automatizadas que possibilitem a localização dos arquivos e a consequente persecução penal dos criminosos[52].

No Brasil, a pornografia infantil e a pedofilia são problemas muito graves e precisam ser adequadamente tratados. Apesar da dificuldade de estabelecer o escopo preciso do problema, é evidente que esses crimes aumentaram significativamente com o estabelecimento da internet[53].

As crianças – a Convenção Sobre os Direitos da Criança (1989) considera criança todo ser humano menor de 18 anos – podem ser enganadas por pessoas que com elas estabelecem contato digital. Normalmente, essas pessoas fingem ser jovens de idade similar para atrair o interesse com assuntos simpáticos às suas potenciais vítimas. Procuram descobrir os pontos de

[50] Hashes são assinaturas de um documento que o deixam distinguíveis de qualquer outro na internet. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes>. Acesso em: 11/05/2020.

[51] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 18. Acesso em: 11/05/2020.

[52] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 18. Acesso em: 11/05/2020.

[53] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 18. Acesso em: 11/05/ 2020.

fragilidade das crianças e se valem disso durante o contato virtual[54].

Contudo, cabe pontuar que o termo pedofilia representa uma doença, desvio de sexualidade ou desordem mental caracterizado pela atração por crianças ou adolescentes, é uma forma de violência sexual, não devendo, portanto, ser confundido com pornografia infantojuvenil. Assim, nem sempre o crime de pornografia infantojuvenil é praticado por pedófilos, considerando o lucro financeiro que as organizações criminosas buscam com essa atividade[55].

Portanto, o pedófilo é a pessoa que possui a doença pedofilia, ao passo que a pornografia infantojuvenil é encontrada em arquivos de vídeos e imagens. A tipificação dos crimes de produção, reprodução, compartilhamento e posse desses arquivos está disposta nos artigos 240 e 241 do Estatuto da Criança e do Adolescente (Lei nº 8.069/1990, alterados pela Lei nº 11.829/2008)[56].

4.1 Pedofilia na Internet: como ocorre?

O aliciamento é um processo aplicado pelo pedófilo para conhecer melhor sua vítima, contatá-la, obter seus dados e preparar a criança para o abuso sexual propriamente dito. Para isso, o pedófilo utiliza os *chats* de conversa na internet, com

[54] INSTITUTO WCF-BRASIL. Navegar com Segurança: protegendo seus filhos da pedofilia e da pornografia infanto-juvenil na internet. São Paulo, CENPEC, 2006, p. 20. Disponível em: < file:///Users/beatrizcadore/Downloads/navegar_com_seguranca.pdf>. Acesso em: 13/05/2020.

[55] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernéticos*. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 18. Acesso em: 11/05/2020.

[56] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernéticos*. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 18. Acesso em: 11/05/2020.

temática infantil ou não, além das redes sociais. Esses indivíduos empregam temas sexuais nas conversas com o intuito de acabar aos poucos com as inibições dos jovens[57].

É comum que o abusador envie e-mail de propagandas atrativas, "iscas" com temas de interesse do público alvo. Pode ainda buscar essa relação fora da rede, pessoalmente, nas escolas, clubes, *lan houses*, dentre outros[58].

Em geral, o pedófilo se aproveita dos dados fornecidos pela própria criança quando colocam inocentemente suas informações nas redes sociais, *sites, chats*. Esses dados servem ao abusador para construir a sua falsa imagem, que será apresentada à vítima[59].

4.2 Compartilhamento de arquivos da pornografia infantojuvenil na Internet

Conforme o artigo 241-A do ECA[60], pornografia infantojuvenil é uma forma de exploração sexual definida pela produção, utilização, exibição, comercialização de material (fotos, vídeos,

[57] INSTITUTO WCF-BRASIL. Navegar com Segurança: protegendo seus filhos da pedofilia e da pornografia infanto-juvenil na internet. São Paulo, CENPEC, 2006, p. 22. Disponível em: < file:///Users/beatrizcadore/Downloads/navegar_com_seguranca.pdf>. Acesso em: 13/05/2020.

[58] INSTITUTO WCF-BRASIL. *Navegar com Segurança: protegendo seus filhos da pedofilia e da pornografia infanto-juvenil na internet.* São Paulo, CENPEC, 2006, p. 22. Disponível em: < file:///Users/beatrizcadore/Downloads/navegar_com_seguranca.pdf>. Acesso em: 13/05/2020.

[59] INSTITUTO WCF-BRASIL. *Navegar com Segurança: protegendo seus filhos da pedofilia e da pornografia infanto-juvenil na internet.* São Paulo, CENPEC, 2006, p. 22. Disponível em: < file:///Users/beatrizcadore/Downloads/navegar_com_seguranca.pdf>. Acesso em: 13/05/2020.

[60] Art. 241-A. 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: (Incluído pela Lei nº 11.829, de 2008).

desenhos) com cenas de sexo explícito com crianças e adolescentes ou imagem de suas partes genitais com a finalidade sexual[61].

Ressalta-se que a simples existência de imagens ou vídeos com esse tipo de conteúdo disponibilizado na web para acesso por qualquer internauta é suficiente para caracterizar o referido delito, irrelevante o efetivo acesso por usuários[62].

A divulgação de arquivos de pornografia infantojuvenil ocorre normalmente via mensagens eletrônica e em conexões que usam compartilhamento nas redes *Peer-to-Peer* (P2P), como E-Mule, Gnutella e Ares Galaxy. Tais ferramentas de compartilhamento eliminam a necessidade de servidor, ou seja, a comunicação entre os computadores é direta e todos os nós interconectados da rede têm responsabilidades equivalentes. Nesse caso, a estratégia de inspecionar os dados hospedados em um servidor torna-se inefetiva[63].

Novas formas de investigação foram criadas, como o programa *Child Protection System*, que efetua uma identificação automática. Todavia, carece de soluções mais avançadas de buscas em redes P2P, principalmente na busca de arquivos que não sejam somente aqueles já catalogados. Essa atualização é importante, pois os criminosos podem modificar os arquivos de

[61] INSTITUTO WCF-BRASIL. *Navegar com Segurança: protegendo seus filhos da pedofilia e da pornografia infanto-juvenil na internet*. São Paulo, CENPEC, 2006, p. 25. Disponível em: < file:///Users/beatrizcadore/Downloads/navegar_com_seguranca.pdf>. Acesso em: 13/05/2020.

[62] MINISTÉRIO PÚBLICO FEDERAL. *Roteiro de Atuação Crimes Cibernéticos*. 2.ª Câmara de Coordenação e Revisão da Procuradoria-Geral da República 3.ª Edição. Brasília, 2016, p. 285. Acesso em: 08/05/2020.

[63] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernéticos*. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 19. Acesso em: 11/05/2020.

forma que impossibilite uma correspondência com bibliotecas da *hash*[64].

Atualmente, a identificação dos suspeitos de pornografia infantojuvenil é feita de diferentes maneiras, além da detecção automática, destaca-se a infiltração de investigadores que estabelecem um contato com os criminosos no mundo digital ou real. Sendo o suspeito identificado, um mandado pode ser obtido para analise e investigação dos dispositivos eletrônicos[65].

A identificação de arquivos de pornografia de crianças é mais fácil que a de adolescentes, tendo em vista um possível desenvolvimento mais rápido do que usual. Isso é mais frequente em adolescentes do sexo feminino, que podem ser confundidas com pessoas adultas, situação comum nos casos de arquivos com menor resolução gráfica[66].

Entretanto, a quantidade de conteúdo com esse teor apenas cresce, deixando cada vez mais vítimas. Para combater tal delito, é necessário aumentar os recursos investidos na persecução penal desses criminosos, o que muitas das vezes não é possível. No entanto, os métodos tradicionais utilizados para investigação também são insuficientes[67].

Dessa forma, se houvesse um investimento mais eficiente e uma ferramenta corretamente desenvolvida, os resultados seriam

[64] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 19. Acesso em: 11/05/2020.

[65] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 19. Acesso em: 11/05/2020.

[66] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 19. Acesso em: 11/05/2020.

[67] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernético*s. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 20. Acesso em: 11/05/2020.

mais positivos. Um exemplo ressaltado pelo Ministério Público Federal, seria a utilização de um método de múltiplas técnicas, como o *multi modal feature fusion* – que utiliza a combinação automática de programas de investigação que diminue o número de arquivos para analise forense[68].

5 CONCLUSÃO

Em face ao exposto, é possível concluir que o desenvolvimento da internet, enquanto meio de comunicação e informação, além dos aspectos positivos no cotidiano da sociedade internacional, resultou em um crescimento exponencial dos números de crimes informáticos. Todavia, cabe aqui uma reflexão, não só em relação as crianças vítimas de violência, mas também a quem comete esses delitos.

A rapidez com que as informações negativas são transmitidas e reproduzidas no mundo digital podem gerar consequências sem dimensões. De igual maneira, ações de educação e prevenção podem ter os mesmos efeitos, desde que estejamos dispostos a fortalecer vínculos saudáveis, entendendo os benefícios dessa nova forma de relação na sociedade moderna, buscando enfrentar a violência no meio digital.

Depreende-se a partir de todas as informações aqui lançadas, que ao facilitar o acesso da sociedade à rede mundial de computadores, mais indivíduos são expostos à pedofilia e à pornografia infantil. O conteúdo que antes era divulgado a um grupo restrito, torna-se hoje alvo fácil de qualquer internauta a qualquer momento, bastando um *click*.

[68] MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernéticos*. Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018, p. 20. Acesso em: 11/05/2020.

A pedofilia e a pornografia infantil são intensamente rejeitadas pela sociedade, ainda que de forma paradoxal essa mesma sociedade gera esses tipos de delitos. Isso demonstra a importância de falar sobre o assunto, com o objetivo de construir meios eficazes de restrição dessas ações criminosas, bem como o fortalecimento das relações interpessoais.

Por fim, é necessário que os governos entendam as mudanças no *modus operandi* dessas atividades delituosas, trabalhando incessantemente em conjunto com as indústrias e universidades para o desenvolvimento de novas tecnologias de investigação, melhorando, assim, os meios tecnológicos disponíveis para combater os delitos analisados. Dessa forma, podemos vislumbrar um ambiente digital mais seguro para as crianças.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. *Cibercrimes e seus Reflexos no Direito Brasileiro*. São Paulo: JusPodivm, 2020, p. 52.

BRITZ, Marjie T. *Computer forensics and cybercrime: an introduction*. New Jersey: Pretice Hall, 2009.

CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais*. 2ed. Rio de Janeiro: Lumen Juris, 2003.

CONTE, Christiany Pegorari; SANTOS, Coriolano Aurélio de Almeida Camargo. *Desafios do Direito Penal no Mundo Globalizado: A Aplicação da Lei Penal no Espaço e os crimes informáticos.* Disponível em: < http://www.oabma.org.br/public/uploads/files/siteComissoes/2017100510283859d63386ebf0a.pdf>. Acesso em: 09/05/2020.

CONVENÇÃO SOBRE O CIBERCRIME. Budapeste, 2011. Disponível em: < http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c7561573570

59326c6864476c3259584d76574339305a58683062334d76634842794d544d794c5668664d53356b62324d3d&fich=ppr132-X_1.doc&Inline=true>. Acesso em: 11/05/2020.

CORREA, Fabiano Simões. *Um estudo qualitativo sobre as representações utilizadas por professores e alunos para significar o uso da internet.* Tese apresentada no Programa de Pós-Graduação em Psicologia da Universidade de São Paulo [USP], sob a orientação do Prof. Sergio Kodato. Ribeirão Preto: USP, 2013.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2017.

CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais: do que estamos falando?* Disponível em: < https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/>. Acesso em: 11/05/2020.

EUFRASIO, Emília Teixeira Lima. *O Cibercrime e a violação dos Direitos Fundamentais de natureza pessoal dos menores.* 100 f. Tese apresentada no Programa de Mestrado em Direito da Universidade Fernando Pessoa, sob a orientação do Professor João Casqueira. Porto: Universidade Fernando Pessoa, 2015.

INSTITUTO WCF-BRASIL. *Navegar com Segurança: protegendo seus filhos da pedofilia e da pornografia infanto-juvenil na internet*. São Paulo, CENPEC, 2006, p. 25. Disponível em: < file:///Users/beatrizcadore/Downloads/navegar_com_seguranca.pdf>. Acesso em: 13/05/2020.

MACHADO, Thiago José Ximenes. *Cibercrime e o crime no mundo informático.* Tese apresentada no Programa de Mestrado em Criminologia da Universidade Fernando Pessoa, sob a orientação da Professora Rita Rola. Porto, 2017.

KESIKOWSKI, Sabrina Cunha; WINTER, Luis Alexandre Carta; GOMES, Eduardo Biacchi. *Atuação do Grupo Mercado Comum frente à criminalidade organizada transnacional.* Revista de Direito Internacional, v. 15, n. 2, p. 353-369, 2018.

MAZONI, Ana Carolina. *Crimes na Internet e a Convenção de Budapeste.* 64 f. Tese apresentada no Programa de Bacharelado em Direito do Centro Universitário de Brasília [Uniceub], sob a orientação do Prof. George Leite. Brasília: UniCEUB, 2009.

MINISTÉRIO PÚBLICO FEDERAL. *Crimes Cibernéticos.* Procuradoria-Geral da República 2.ª Câmara de Coordenação e Revisão. Coletânea de Artigos, Vol. 3. Brasília: 2018.

MINISTÉRIO PÚBLICO FEDERAL. *Roteiro de Atuação Crimes Cibernéticos.* 2.ª Câmara de Coordenação e Revisão da Procuradoria-Geral da República 3.ª Edição. Brasília, 2016.

PAIVA, Mário Antônio Lobato de. *Os institutos do Direito Informático*. Âmbito Jurídico, Rio Grande, VI, n. 14, 2003. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-14/os-institutos-do-direito-informatico/>. Acesso em: 11/05/2020.

ROSSINI, Augusto Eduardo de Souza. *Brevissímas considerações sobre delitos informáticos.* Caderno Jurídico, Ano 2, n. 4, 2002, p. 133-142. Disponível em: < http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Cadernos_Tematicos/direito_e_internet.pdf>. Acesso em: 11/05/2020.

SILVA, João Miguel Almeida da. *Cibercrime: O Crime de Pornografia Infantil na Internet.* 57 f. Tese apresentada no Programa de Mestrado em Direito da Universidade de Coimbra, sob a orientação da Prof. Ana Rita da Silva Samelo Alfaiate. Coimbra: Universidades de Coimbra, 2016.

Tutorial Teleco. *Internet no Brasil – Perfil dos usuários*. Disponível em: < https://www.teleco.com.br/internet_usu.asp>. Acesso em: 07/05/2020.

O CRIME ORGANIZADO E O USO DE CRIPTOMOEDAS

Felipe Tonissi Lipelt[1]

RESUMO

As moedas digitais vêm ganhando destaque nos últimos anos e possuem um papel de destaque nas atividades ilegais devido à alta complexidade da matéria. O desafio para a criação de mecanismos de investigação e know-how da atuação da criminalidade cibernética apresentam um grande desafio para pesquisadores e entidades buscam o combate aos crimes cibernéticos. Realmente trata-se de um problema expressivo no qual escala total de uso indevido de moedas virtuais seja desconhecida, seu valor de mercado chegou a superar a marca de 7 bilhões de euros em todo o mundo. O presente artigo busca tratar sobre esse fenômeno de uma perspectiva jurídica, com foco no uso de criptomoedas para crimes financeiros, como lavagem de dinheiro.

Palavras-chave: Criptomoedas. Crimes cibernéticos. Investigação.

ABSTRACT

Digital currencies have been gaining prominence in recent years and have a prominent role in illegal activities due to the high complexity of the matter. The challenge for the creation of

[1] Advogado. Bacharel em direito pelo Centro Universitário de Brasília. Aluno do curso de pós graduação *lato sensu* do Instituto Ceub de Pesquisa e Desenvolvimento – UniCEUB/ICPD.

investigation mechanisms and know-how of the performance of cyber crime presents a great challenge for researchers and entities seeking to combat cyber crimes. It is really a significant problem in which the total scale of misuse of virtual currencies is unknown, its market value has even surpassed the mark of 7 billion euros worldwide. This article seeks to address this phenomenon from a legal perspective, focusing on the use of cryptocurrencies for financial crimes, such as money laundering and tax evasion, in addition to financing terrorism.

Keywords: Cryptocurrencies. Cyber crimes. Investigation.

1 INTRODUÇÃO

As criptomoedas trouxeram ao mundo moderno uma forma inédita de transação de valores em níveis mundial, isto é, não há a necessidade de um órgão gestor central.

As facilidades de aquisição e a funcionalidade das moedas universais digitais remodelaram as relações comerciais que habitualmente ocorriam no meio virtual. Contudo, a forma em que as criptomoedas são adquiridas e utilizadas, facilitam com que empresas e organizações pratiquem ilícitos penais e tributários ao mascarar transações com "dinheiro sujo" dando uma falsa aparência de licitude, a denominada lavagem de dinheiro.

Isto se dá porque a gestão, criação e circulação das criptomoedas não possuem qualquer meio de fiscalização ou supervisão por órgãos regulamentadores. Assim, facilitando para que os criminosos possam procurar sites de câmbio ou usuários independentes que desejem comercializar as moedas e então, revestirem o dinheiro ilícito de uma vestimenta neutra.

Com a crescente popularidade do mercado de criptomoedas, governos e outras partes interessadas ao redor do mundo tem dado maior atenção ao grande número de moedas cibernéticas não regulamentadas. Para que se possa ter uma maior dimensão, em

2018, presumia-se que a capitalização de mercado total das 100 maiores criptomoedas excedesse o equivalente a 330 bilhões de euros ao redor mundo[2].

A capitalização de mercado total de todas as criptomoedas juntas naquele período atingiu um pico ainda maior, chegando à casa dos US$ 728 bilhões, caindo apenas três semanas depois, para aproximadamente US$ 360 bilhões[3].

2 CRIPTOMOEDAS E BLOCKCHAIN

Não é tarefa fácil determinar o conceito de criptomoeda. As criptomoedas se tornaram uma palavra de ordem para se referir a uma ampla gama de desenvolvimentos tecnológicos que utilizam uma técnica mais conhecida como criptografia.

Em termos simples, a criptografia é a técnica de proteger as informações, transformando-as (ou seja, criptografando-as) em um formato ilegível que só pode ser decifrado (ou descriptografado) por alguém que possua uma chave secreta. As criptomoedas como o Bitcoin são protegidas por esta técnica usando um sistema engenhoso de chaves digitais públicas e privadas [4]

[2] European regulators warn on cryptocurrency risks. [Internet]. Finextra. [acessado em 18 mai. 2020]. Disponível em: https://www.finextra.com/pressarticle/72597/european-regulators-warn-on-cryptocurrency-risks

[3] R.M. BRATSPIES, "Cryptocurrencies and the Myth of the Trustless Transaction", March 2018, 6-7 [acessado em 18 mai. 2020]. Disponível em: https://ssrn.com/abstract=3141605.

[4] Cryptocurrencies and blockchain. HOUBEN, Dr. Robby e SNYERS, Alexander. 2018. P. 16.

Para melhor exemplificar as criptomoedas, podemos citar o bitcoin, que é o principal exemplo e é considerada a primeira moeda digital que dispensa uma autoridade central de controle[5].

Apesar do conceito de criptomoeda estar relacionado a uma moeda (dinheiro), o real valor das moedas cibernéticas fica guardado na chamada "transação", dessa forma, os valores pertencentes a um detentor da criptomoeda não ficam essencialmente em sua carteira digital, mas sim na representação das transações que originaram aquele valor[6].

O Professor Fernando Ulrich[7] nos traz um exemplo prático de uma transação por meio de bitcoins:

> Quando a Maria decide transferir bitcoins ao João, ela cria uma mensagem, chamada de "transação", que contém a chave pública do João, assinando com sua chave privada. Olhando a chave pública da Maria, qualquer um pode verificar que a transação foi de fato assinada com sua chave privada, sendo, assim, uma troca autêntica, e que João é o novo proprietário dos fundos.

Isto é, as transações funcionam como uma espécie de cadeia de assinaturas digitais. As transações são transferidas de proprietário para proprietário por meio de uma assinatura digital, um hash (transformação de uma grande quantidade de dados em uma pequena quantidade de informações) da operação anterior e a

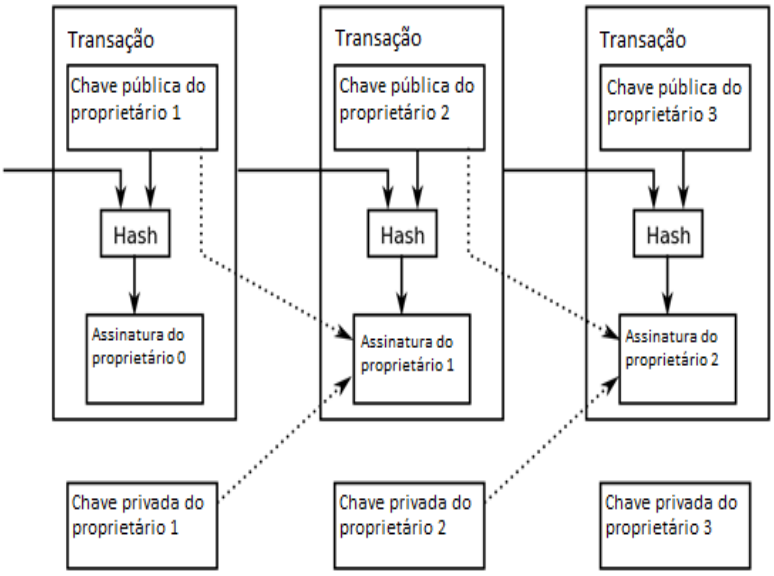
[5] A brief history on Bitcoin & Cryptocurrencies. Ledger Academy. [acessado em 23 mai. 2020]. Disponível em: https://www.ledger.com/academy/crypto/a-brief-history-on-bitcoin-cryptocurrencies#:~:text=Ten%20years%20ago%2C%20Bitcoin%20emerged,events%20during%20this%20time%20period.

[6] Cryptocurrencies and blockchain. HOUBEN, Dr. Robby e SNYERS, Alexander. 2018. P. 17.

[7] ULRICH, Fernando. Bitcoin a Moeda na Era Digital. Mises Brasil. São Paulo, 2014. p. 18.

chave pública do próximo proprietário, adicionando-os para o final da moeda[8].

Figura 1: Imagem ilustrativa do hash



Fonte: Blockgeeks, 2017.

O blockchain, por sua vez, é um tipo específico (ou subconjunto) da chamada tecnologia de contabilidade distribuída ("Distributed Ledger Technology - DLT")[9]. O DLT é uma maneira de registrar e compartilhar dados em vários repositórios de dados (também conhecidos como livros contábeis), cada um com exatamente os mesmos registros de dados, sendo estes mantidos

[8] What Is Hashing? [Step-by-Step Guide-Under Hood Of Blockchain]. [Internet]. Blockgeeks. [acessado em 18 mai. 2020]. Disponível em: https://blockgeeks.com/guides/what-is-hashing/#:~:text=In%20simple%20terms%2C%20hashing%20means,output%20of%20a%20fixed%20length.

[9] Another example of distributed ledger technology is "directed acyclic graph", the underlying technology of the IOTA-platform. M. VAN DE LOOVERBOSCH, "Crypto-effecten: tussen droom en daad", TRV-RPS 2018, 193, nota de roda-pé n° 2.

e controlados coletivamente por uma rede distribuída de servidores de computador, denominados "nós"[10].

Trata-se, então, de um mecanismo que emprega um método de criptografia, utilizando-se um conjunto de algoritmos matemáticos específicos para criar e verificar uma estrutura de dados em crescimento contínuo - à qual os dados só podem ser adicionados e dos quais os dados existentes não podem ser removidos - formando uma cadeia de "blocos de transações", que funciona como um livro de contabilidade distribuído[11].

Em termos simples, o blockchain pode ser pensado como um banco de dados distribuído. As adições a esse banco de dados são iniciadas por um dos membros (os nós da rede), que cria um novo "bloco" de dados, que pode conter todos os tipos de informações. Esse novo bloco é então transmitido para todas as partes da rede de forma criptografada, para que os detalhes da transação não sejam divulgados publicamente. Os membros da rede (os outros nós da rede) determinam coletivamente a validade do bloco de acordo com um método de validação algorítmica predefinido. Uma vez validado, o novo "bloco" é adicionado ao blockchain, o que resulta essencialmente em uma atualização do livro de contabilidade de transações que é distribuído pela rede[12].

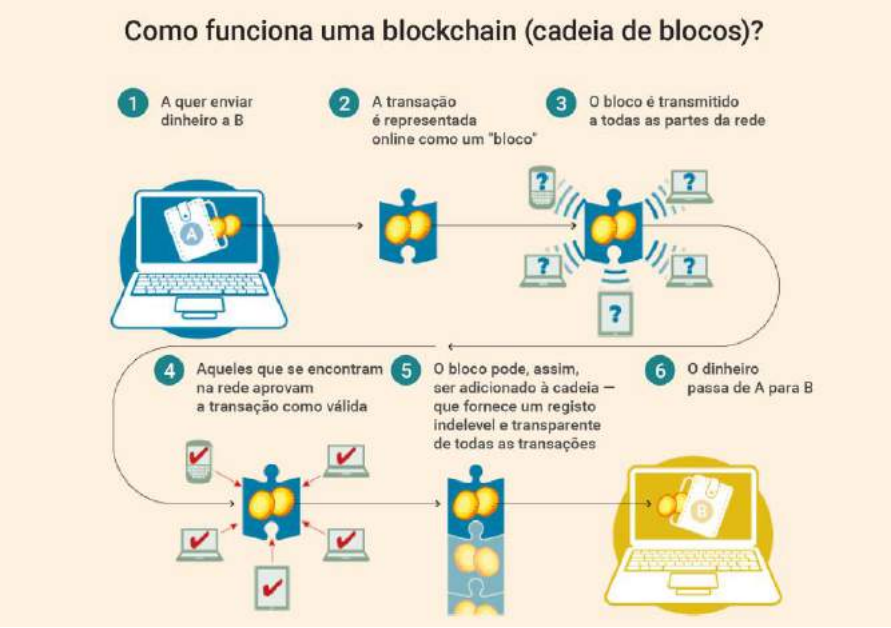
Veja a ilustração abaixo para melhor compreensão.

[10] World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, nota da FinTech n° 1. Washington, D.C., [acessado em 18 mai. 2020]. Disponível em: http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf e CPMI, "Digital currencies", Novembro de 2015, [acessado em 18 mai. 2020]. Disponível em: https://www.bis.org/cpmi/publ/d137.pdf.

[11] Cryptocurrencies and blockchain. HOUBEN, Dr. Robby e SNYERS, Alexander. 2018. P. 16.

[12] Cryptocurrencies and blockchain. HOUBEN, Dr. Robby e SNYERS, Alexander. 2018. P. 16.

Imagem 2: Como funciona uma blockchain.



Fonte: Technology: Banks seeks the key to blockchain

Como já dito, uma das principais vantagens da tecnologia blockchain é que ela permite simplificar a execução de uma ampla variedade de transações que normalmente exigiriam a intermediação de terceiros (por exemplo, um custodiante, um banco, um sistema de liquidação de valores mobiliários, corretoras, repositório de transações,…). Em essência, o blockchain tem tudo a ver com descentralizar a confiança e permitir a autenticação descentralizada das transações.

3 O USO DAS CRIPTOMOEDAS PELOS CRIMINOSOS

Não resta dúvidas de que a criação das criptomoedas são frutos de uma revolução na forma de lidar e tratar do dinheiro. Grande parte dessa transformação se explica em pela funcionalidade, facilidade e aparente segurança que o ambiente virtual tem trago a seus usuários6. Ao passar dos dias, a interação

com as instituições financeiras tem se simplificado. Já não é mais necessário ir a uma agencia bancaria para criar uma conta corrente, por exemplo.

Em consonância a esta revolução, há o surgimento de novas práticas delituosas, as quais em um primeiro momento causa estranheza e confusão. Veja por exemplo o caso em que um sujeito sequestrou duas mulheres e exigiu o pagamento do resgate em bitcoin[13]. Ações como esta não são exclusividade do Brasil, tendo ocorrido situações similares em outros países[14,15,16].

Como já referenciado no título anterior, o Bitcoin é descentralizado, o que faz com que ele não dependa de um banco ou órgão de fiscalização, sendo o próprio software o responsável pelo o estabelecimento das regras de funcionamento da criptomoeda, sendo projetado para que seus próprios usuários a controlem.

Contundo, a inovação tecnológica e liberativa trazida pelas criptomoedas não possui um alinhamento com os órgãos de controle e fiscalização. Perceba que ao passo que temos o surgimento de uma nova maneira de realizar pagamentos e transferências de uma moeda considerada pelos próprios usuários

[13] Sequestrador pede R$ 8 milhões em bitcoin para liberar mulheres. [Internet]. Jornal de Brasília. [acessado em 9 mai. 2020]. Disponível em: https://jornaldebrasilia.com.br/cidades/sequestrador-pede-r-8-milhoes-em-bitcoin-para-liberar-mulheres/

[14] Cryptocurrency Ransom Demanded for Wife of Norwegian Tycoon. [Internet]. The New York Times. [acessado em 9 mai. 2020]. Disponível em: https://www.nytimes.com/2019/01/10/world/europe/norway-kidnapping-monero.html

[15] Ukraine kidnappers free bitcoin analyst after $1 mln ransom paid. [Internet]. Reuters. [acessado em 9 mai. 2020]. Disponível em: https://www.reuters.com/article/us-ukraine-kidnapping/ukraine-kidnappers-free-bitcoin-analyst-after-1-mln-ransom-paid-idUSKBN1EN1QB

[16] Indian Businessman Kidnapped For Bitcoin. [Internet]. Reuters. [acessado em 9 mai. 2020]. Disponível em: https://www.investopedia.com/news/indian-businessman-kidnapped-bitcoin/

com o mesmo conceito que tem o papel-moeda, no entanto, não é reconhecido como dinheiro para o governo.

Essa grande área obscura que a falta de regulamentação traz às criptomoedas, torna o cenário favorável ao cometimento de ilícitos penais, em especial a lavagem de dinheiro.

Sabe-se que o crime de lavagem de dinheiro é uma prática delituosa em que se pratica um conjunto de atos para disfarçar a natureza, origem, localização, disposição, movimentação ou propriedade de bens, valores ou direitos originados de forma criminosa ou contravencional, com o fim de realocação na economia, com aspecto de lícito[17].

A Lei nº 9.613, de 3 de março de 1998, alterada pela Lei nº 12.683, de 9 de julho de 2012, em seu artigo 1º, §1º e em seu artigo 9º estabelece que é considerado crime de "lavagem ou ocultação de bens, direitos e valores", converter ativos ilícitos em lícitos; adquirir, receber, trocar, transferir, manter como garantia, movimentar ou transferir; importar ou exportar bens com valores não correspondentes aos verdadeiros.

Os juristas Pierpaolo Cruz Bottini e Gustavo Henrique Badaró[18] definem a lavagem de dinheiro da seguinte forma: "Trata-se, em suma, do movimento de afastamento dos bens de seu passado sujo, que se inicia com a ocultação simples e termina com a introdução no circuito comercial ou financeiro, com aspecto legítimo".

[17] Lavagem de dinheiro: Esconder a origem de recursos ilegais é crime. [Internet]. Tribunal de Justiça do Distrito Federal e Territórios. [acessado em 18 mai. 2020]. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/lavagem-de-dinheiro

[18] BOTTINI, Pierpaolo Cruz; BADARÓ, Gustavo Henrique. Lavagem de dinheiro: aspectos penais e processuais penais: comentários à Lei 9.613/1998, com as alterações da Lei 12.683/2012. São Paulo: Editora Revista dos Tribunais, 2012. Cap. 1, p. 21.

Assim, o início da páatica delituosa consiste na prática de uma infração penal e a consequente ocultação dos valores ilícitos auferidos. Subsequentemente, desenvolve-se operações para disfarçar a origem dos bens, concluindo-se com a reinserção do dinheiro auferido ilicitamente na economia, contudo desta vez com o ar de aparência lícita.

Desta forma, temos que as "fases" da lavagem de dinheiro tem como propósito, distanciar o recurso financeiro da fonte, dificultar a vinculação direta com o ato ilícito; encobrir as várias formas de movimentações para atrapalhar o rastreamento do dinheiro e; por fim, retornar o dinheiro a origem de forma limpa[19].

Sabe-se que o objeto material é aquele sobre o qual recai o comportamento ilícito[20], não se embaraçando, na maior parte das vezes, com o bem jurídico tutelado pela lei penal. De acordo com a Convenção de Palermo, integralizado pelo ordenamento jurídico brasileiro por meio do Decreto nº. 5.015, de 12 de março de 2005, dispõe em seu artigo 2°, alínea "d" que bens são:

> Artigo 2
>
> Terminologia
>
> Para efeitos da presente Convenção, entende-se por:
>
> (...);
>
> d) "Bens" - os ativos de qualquer tipo, corpóreos ou incorpóreos, móveis ou imóveis, tangíveis ou intangíveis, e os documentos ou instrumentos jurídicos que atestem a propriedade ou outros direitos sobre os referidos ativos;

Outrossim, temos que os bens passíveis de lavagem são todos aqueles que advêm, direta (producta sceleris) ou

[19] MINK, Gisela Fernandes Cardoso. Lavagem de dinheiro. 2005. 58 f. Monografia (Graduação) – Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2005.

[20] BITENCOURT, Cezar Roberto. Tratado de Direito Penal - Econômico - Volume 2. Saraiva Educação S.A., 6 de out. de 2017.

indiretamente (fructus sceleris), do ilícito penal. Os bens diretamente provenientes têm ligação imediata com o crime anterior, enquanto os indiretamente são resultado de uma transformação ou substituição dos bens anteriores[21].

Veja que de forma exemplificativa, podemos apontar a Operação "Pão Nosso", em que a Polícia Federal do Rio de Janeiro encontrou provas de que um esquema de lavagem de dinheiro estava começando a utilizar Bitcoin para esconder valores desviados dos cofres públicos[22]. O suposto esquema funcionava na Secretaria de Administração Penitenciária do RJ, através de um contrato para fornecimento de pães para os presos em penitenciárias do estado.

O Superintendente Adjunto da Receita Federal no Rio, explicou que dos R$ 73 milhões desviados com o contrato de fornecimento de pães, R$ 300 mil foram transformados em Bitcoin. A intenção dos criminosos seria recuperar o dinheiro no exterior[23].

Desta forma, percebe-se que as criptomoedas, por suas propriedades únicas, que permitem citar a utilização de pseudônimo por seus usuários, bem como a falta de controle por parte do governo sobre sua emissão e circulação, permite com facilidades que se tornem objeto material do crime de lavagem de dinheiro.

[21] ANJOS, Alexandre Bispo dos; e SILVA, Jacqueline Oliveira. Bitcoin como objeto material do crime de lavagem de dinheiro. 2014.

[22] Esquema de fraude no sistema penitenciário do RJ usou bitcoin para lavar dinheiro, diz Receita. [Internet]. Globo. [acessado em 18 mai. 2020]. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/pf-detalha-esquema-do-pao-nosso-que-prendeu-delegado-e-ex-secretario-de-sergio-cabral.ghtml

[23] Esquema de fraude no sistema penitenciário do RJ usou bitcoin para lavar dinheiro, diz Receita. [Internet]. Globo. [acessado em 18 mai. 2020]. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/pf-detalha-esquema-do-pao-nosso-que-prendeu-delegado-e-ex-secretario-de-sergio-cabral.ghtml

4 CONCLUSÃO

O objetivo do presente artigo foi tratar sobre o fenômeno das criptomoedas de uma perspectiva jurídica, com foco no uso destas moedas para crimes financeiros, como o da lavagem de dinheiro.

Cumpre-me destacar que um dos principais pontos achados durante a pesquisa para a confecção deste artigo foi a variedade de empresas que aceitam receber Bitcoins como, sendo veiculado no final do ano de 2019 que a empresa CIELO teria passado a aceitar o Bitcoin16. A variedade de empresas que aceitam o Bitcoin possibilita uma diversidade de bens e serviços que podem ser gozados com recursos supostamente provenientes de crimes.

Diante da ausência de legislação que regulamenta a compra, a manutenção, o registro, a tributação, a emissão, o controle de criptomoedas, verificou-se também a ausência de atuação de órgãos de controle para cyber moedas.

Certo é que a tecnologia atua em ambos os lados da inovação, sendo que a cada novo avanço tecnológico, tanto o lado das autoridades quanto a dos criminosos tende a inovar. É necessário a elaboração de estruturas que avalizem a privacidade dos cidadãos, mas que ao mesmo tempo garanta a proteção dos crimes.

REFERÊNCIAS

Another example of distributed ledger technology is "directed acyclic graph", the underlying technology of the IOTA-platform. M. VAN DE LOOVERBOSCH, "Crypto-effecten: tussen droom en daad", TRV-RPS 2018, 193, nota de roda-pé n° 2.

ARABINDA, Acharya. Targeting Terrorist Financing: International Cooperation and New Regimes, Nova Iorque: Routledge, 2009.

BITENCOURT, Cezar Roberto. Tratado de Direito Penal - Econômico - Volume 2. Saraiva Educação S.A., 6 de out. de 2017.

BOTTINI, Pierpaolo Cruz; BADARÓ, Gustavo Henrique. Lavagem de dinheiro: aspectos penais e processuais penais: comentários à Lei 9.613/1998, com as alterações da Lei 12.683/2012. São Paulo: Editora Revista dos Tribunais, 2012. Cap. 1, p. 21.

CAMARA, Michele Pacheco. O Bitcoin é alternativa aos meios de pagamento tradicionais? 2014. 76 f. Monografia (Graduação), Escola de Administração da Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

Cielo fecha parceria com startup Bitfy para aceitar pagamentos com Bitcoin. [Internet]. Valor. [acessado em 23 mai. 2020]. Disponível em: https://valor.globo.com/financas/noticia/2019/12/27/cielo-fecha-parceria-com-startup-bitfy-para-aceitar-pagamentos-com-bitcoin.ghtml

Cryptocurrency Ransom Demanded for Wife of Norwegian Tycoon. [Internet]. The New York Times. [acessado em 9 mai. 2020]. Disponível em: https://www.nytimes.com/2019/01/10/world/europe/norway-kidnapping-monero.html

European regulators warn on cryptocurrency risks. [Internet]. Finextra. [acessado em 18 mai. 2020]. Disponível em: https://www.finextra.com/pressarticle/72597/european-regulators-warn-on-cryptocurrency-risks

Indian Businessman Kidnapped For Bitcoin. [Internet]. Reuters. [acessado em 9 mai. 2020]. Disponível em: https://www.investopedia.com/news/indian-businessman-kidnapped-bitcoin/

MINK, Gisela Fernandes Cardoso. Lavagem de dinheiro. 2005. 58 f. Monografia (Graduação) – Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2005.

OFTEDAL, Emilie, The Financing of Jihadi Terrorist Cells in Europe, Norway: Forsvarets Forskningsinstitutt, January 6, 2015.

R.M. BRATSPIES, "Cryptocurrencies and the Myth of the Trustless Transaction", March 2018, 6-7 [acessado em 18 mai. 2020]. Disponível em: https://ssrn.com/abstract=3141605.

Sequestrador pede R$ 8 milhões em bitcoin para liberar mulheres. [Internet]. Jornal de Brasília. [acessado em 9 mai. 2020].

Disponível em:
https://jornaldebrasilia.com.br/cidades/sequestrador-pede-r-8-milhoes-em-bitcoin-para-liberar-mulheres/

Ukraine kidnappers free bitcoin analyst after $1 mln ransom paid. [Internet]. Reuters. [acessado em 9 mai. 2020]. Disponível em: https://www.reuters.com/article/us-ukraine-kidnapping/ukraine-kidnappers-free-bitcoin-analyst-after-1-mln-ransom-paid-idUSKBN1EN1QB

ULRICH, Fernando. Bitcoin a Moeda na Era Digital. Mises Brasil. São Paulo, 2014. p. 18.

World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, nota da FinTech n° 1. Washington, D.C., [acessado em 18 mai. 2020]. Disponível em: http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf e CPMI, "Digital currencies", Novembro de 2015, [acessado em 18 mai. 2020]. Disponível em: https://www.bis.org/cpmi/publ/d137.pdf.

TIPIFICAÇÃO DA DIVULGAÇÃO DE NOTÍCIAS FALSAS NO MEIO DIGITAL: A POSSIBILIDADE DA PERSECUÇÃO PENAL DOS AUTORES E A PONDERAÇÃO FRENTE AO PRINCÍPIO DA LIVRE

Tiago Ridek Yamaguchi[1]

RESUMO

O presente trabalho, busca analisar juridicamente a questão da divulgação de notícias falsas, fato que teve expressivo aumento na última década, em razão da facilidade de propagação de notícias perpetrada pelo crescente aumento do uso das redes sociais pela população mundial. Inicialmente, conceitua e expõe a classificação dos principais tipos de notícias falsas. Pondera-se a questão da regulação das fake words frente ao princípio constitucional da liberdade de expressão, em razão do temor de se resultar em ações que suprimam a livre manifestação das pessoas. Apresenta-se, em apertada síntese, questões acerca da categorização das notícias falsas, a fim de se entender melhor a possibilidade de se buscar a responsabilização penal de pessoas que se dedicam a este tipo de atividade com o intuito de alcançar objetivos socialmente lesivos.

Palavras-chave: Fake words. Liberdade de expressão. Tipificação penal.

ABSTRACT

This scientific article seeks to analyze legally the question of spreading false news, fact that has increased significantly in the

[1] Advogado atuante na área de Direito Público. Bacharel em Direito pelo Centro Universitário de Brasília - UniCEUB. Aluno da pós-graduação lato sensu do Instituto Ceub de Pesquisa e Desenvolvimento – UniCEUB/ICPD.

last decade, caused by the ease of spreading news perpetrated by the real increase in the use of social networks by the world population. Initially, it conceptualizes and exposes a classification of the main types of fake news. The question of the application of false words is considered in view of the constitutional principle of freedom of expression, due to the fear of causing actions that suppress the free manifest of people. It presented in synthesis issues related to the categorization of false news, in order to better understand the possibility of seeking criminal liability for people who dedicate themselves for a type of activity in order to achieve harmful social objectives.

Keywords: Fake words. Freedom of expression. Penal typification.

1 INTRODUÇÃO

Trata-se de tema atual, que, em razão das inúmeras consequências causadas pela rápida proliferação de notícias falsas, impulsionadas pela facilidade que as redes sociais e a facilidade de se criar e manter portais divulgadores de notícias. Tal conduta causa altera a forma como se entende as notícias, resultando em impacto profundo na sociedade de uma forma geral.

Há de se ressaltar que o direito pátrio possui um código penal cuja criação se deu no ano de 1940, momento em que a ideia de uma rede mundial de computadores poderia ser considerada apenas uma previsão tecnológica de alguma obra de ficção científica. Este fato faz com que a discussão sobre a penalização de atitudes perpetradas em meios digitais divida opiniões. Alguns acreditam que há a necessidade de uma revisão do código para que se possibilite a criação de tipos penais que se amoldem à realidade atual, outros creem que isso pode gerar um excesso por parte do estado em relação ao direito penal, resultando em violação ao princípio da proporcionalidade. Outro ponto muito importante relacionado à criminalização da publicação dolosa de informações falsas é o fato do respeito ao princípio

constitucional da livre manifestação do pensamento ou liberdade de expressão.

O Direito Penal é um ramo da ciência jurídica que tem como uma de suas tarefas precípuas a discussão e proposição de medidas que coíbam ou reduzam os danos relacionados a atividade socialmente indesejáveis (regulação social), a fim de proteger bens jurídico de extrema importância. Nesse caso, a questão da divulgação das notícias falsas tornou-se grande protagonista das discussões dessa área jurídica, sendo também muito discutido em relação às matérias de direito civil e constitucional.

A divulgação de notícias falsas tem um grande impacto social, com suspeitas inclusive de que o uso desta ferramenta interferiu diretamente nas eleições norte-americanas de 2016[2]. Em razão do grande impacto que tais ações tiveram em processos eleitorais, o Tribunal Superior Eleitoral-TSE promoveu debates acerca do tema em algumas ocasiões, inclusive em 2017, antes das eleições de 2018. No ano de 2019, o TSE divulgou resolução normatizando a questão das propagandas eleitorais das eleições municipais de 2020, em que expressamente prevê punições pela divulgação de informações falsas em propagadas dos candidatos. A resolução nº 23.610, de 2019: [3]

> Art. 27. É permitida a propaganda eleitoral na internet a partir do dia 16 de agosto do ano da eleição (Lei n° 9.504/1997, art. 57-A).
>
> § 1º A livre manifestação do pensamento do eleitor identificado ou identificável na internet somente é passível de limitação quando ofender a honra ou a imagem de candidatos, partidos ou

[2] OLIVEIRA, André Soares; GOMES, Patrícia Oliveira. OS LIMITES DA LIBERDADE DE EXPRESSÃO: FAKE NEWS COMO AMEAÇA A DEMOCRACIA. R. Dir. Gar. Fund., Vitória, v. 20, n. 2, p. 93-118, maio/agosto, 2019

[3] BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Resolução nº 23.610, de 18 de dezembro de 2019. Disponível em: <https://bityli.com/Itp81 >. Acesso em: 02 jun. 2020.

> coligações, ou divulgar fatos sabidamente inverídicos
>
> § 2º O disposto no § 10 deste artigo se aplica, inclusive, às manifestações ocorridas antes da data prevista no caput, ainda que delas conste mensagem de apoio ou crítica a partido político ou a candidato, próprias do debate político e democrático.

É importantíssimo que haja uma preocupação acerca do impacto que a divulgação de notícias falsas causa nos pleitos eleitorais, no entanto, a regulação restrita a esse âmbito torna-se demasiadamente restrita. Não cabe punição expressa que extrapole o âmbito eleitoral, nesse sentido quais seriam as formas de se responsabilizar as demais pessoas que divulgam notícias falsas?

Ademais é difícil a tarefa de encontrar um meio termo entre o excesso de penalização, a ponderação da liberdade de expressão e a possibilidade da punição penal dos responsáveis pela divulgação dolosa de informações inverídicas que causem danos.

2 BREVE ANÁLISE ACERCA DAS MODALIDADES DE NOTÍCIAS FALSAS

2.1 Conceituação de notícias falsas

O surgimento da divulgação de fatos falsos não possui uma data específica de surgimento, é possível inclusive que informações falsas tenham origem simultânea ao surgimento da própria sociedade. A propagação de notícias falsas intencionalmente, a fim de obter algum objetivo não se remete a uma data tão distante. Nesse sentido, é importante que se faça uma análise mais cuidadosa acerca da divulgação de notícias falsas.

Com o advento da internet, potencializada pelo surgimento das redes sociais, houve um crescimento considerável de veículos

digitais de informação. Estes novos veículos nem sempre se apresentam de forma organizada e estruturada, como emissoras ou redes de comunicação, mas sim como portais de informação formados por cidadãos jornalistas[4]. Estes meios utilizam-se de algoritmos para a indicação de conteúdo aos usuários para alcançar o maior número de pessoas com interesse nesses assuntos, o que gera uma espécie de bolha da informação. Este ponto torna-se preocupante, haja vista o agravamento dessa situação no contexto mundial, em que a reascensão de ideais eugenistas e ultraconservadores ganham tanto espaço[5].

Os portais criados por cidadãos tendem a não possuir uma responsabilidade tão grande em relação à checagem de fatos, alia-se a isto o fato de, principalmente no Brasil, haver uma grande polarização política que, em razão do funcionamento de algorítimos, restringe o acesso da população a fatos que seja divergentes ao seu ponto de vista. O resultado disso, muitas vezes, é uma notícia se tornar tão popular e replicada, que se eleva ao status de fato para uma parcela da população que não foi exposta a informações que divirjam da primeira.

Dessa forma, pode ocorrer uma precarização da divulgação de informação, que deriva da ausência de uma revisão ou uma checagem dos fatos antes da publicação. Uma vez publicada, a replicação da notícia pode ocorrer em um curtíssimo espaço de tempo, tornando hercúleo o trabalho de expor as inconsistências ou ausência de veracidade dessas notícias, em razão da dificuldade

[4] Tandoc, Edson & Lim, Zheng & Ling, Rich. (2017). Defining "Fake News": A typology of scholarly definitions. Digital Journalism. 1-17. 10.1080/21670811.2017.1360143. Disponível em:<https://bityli.com/tsb2R >. Acesso em 02 de jun. de 2020.

[5] OLIVEIRA, André Soares; GOMES, Patrícia Oliveira. OS LIMITES DA LIBERDADE DE EXPRESSÃO: FAKE NEWS COMO AMEAÇA A DEMOCRACIA. R. Dir. Gar. Fund., Vitória, v. 20, n. 2, p. 93-118, maio/agosto, 2019

de se checar qual a origem da informação e os dados que a sustentam. Portanto, é de extrema importância que as questões de *fact checking* sejam consideradas como ferramenta essencial aos meios de divulgação de notícias, tanto pelos grandes emissores quanto pelos cidadãos jornalistas, que devem ter a responsabilidade pelo conteúdo que divulgam.

2.2 Tipos de Notícias falsas

A classificação de notícias falsa é importante para se determinar quais serão as consequências jurídicas aplicadas aos propagadores destas.

É comum, em razão dos acontecimentos relacionados à divulgação de notícias falsas por setores políticos, a generalização do termo *fake news*, que passa a ser usada para denominar todo tipo de notícias falsas. Ocorre que as *fake news* estão contidas em um gênero denominado *fake words*, que pode ser resumida no ato de se construir uma informação que não corresponde à realidade, utilizando-se de imagens ou palavras maliciosas, a fim de produzir desinformação a uma pessoa, um grupo ou toda a sociedade. Dentre as *fake words, os tipos mais comuns são: a) Fake news; b) Fictitious entry ou Mountweazel; c) Fake Science; e d) Fake Profile*[6].

[6] ALVES, F. B. ; CORREA, E. A. A. . Análise das redes de relações sociais e o controle jurídico de fake words. In: Fabrício Polido, Lucas Anjos e Luíza Brandão. (Org.). Políticas, internet e sociedade. 1ed.Belo Horizonte: IRIS, 2019, v. 1, p. 158-169.

2.1.1 Fake news

As Fake news são notícias falsas, mas que são criadas por meio de artifícios que as fazem parecer verdadeiras.[7] É comum que se utilize desse artifício para difamar ou prejudicar adversários políticos, ou mesmo para obter vantagem financeira. Portais de notícias falsas utilizam o *adsense* do Google para gerar receita, podendo ser, a depender do volume de acessos do site, um meio muito lucrativo para quem divulga as notícias. Nesse caso, o Google exibe no sítio o anúncio que gerar mais receita[8]. Portanto, um site que tenha um volume grande de acesso pode render valores expressivos, pois os anúncios tornam-se mais onerosos a depender do tráfego de acessos do site.

Esta modalidade é a que tem atraído maior atenção dos estudiosos de diversas áreas das ciências humanas, em razão da sua grande utilização por políticos para propagar mentiras que beneficiem a ascensão de candidatura ou para difamar adversários, prejudicando a campanha ou a imagem destes. Em razão da velocidade com que se propagam por meio das redes sociais, a checagem dos fatos dessas notícias muitas vezes é tardia, ocorrendo após a replicação massiva da informação inverídica. Talvez isso ocorra em razão da vontade que as pessoas têm de contar uma novidade, especialmente sobre algo pelo qual

[7] SOBRAL, Cristiano. A responsabilidade civil dos provedores e de terceiros pelas fake News. Disponível em: <encurtador.com.br/BLYZ6>. Acesso em: 02 jun. 2020.

[8] Adsense do Google. Disponível em: <https://www.google.com.br/adsense/start/> Acesso em 02 de junho de 2020.

se espera uma aceitação dentro das suas respectivas bolhas, onde se opera certa validação digital[9].

2.1.2 Fictious entry ou Mountweazel

As fictious entry, ou Mountweazel, é uma técnica em que expressões ou sinais em determinados trabalhos científicos, verbetes ou mapas, com a intenção de rastrear futuros plágios.[10] Como exemplo de plataforma que permite esse tipo de conduta podemos citar o site *Wikipedia*, tipo de enciclopédia virtual que é alimentada por informações inseridas pelos próprios usuários.

Nesse caso, são inseridas falsas informações no meio, gerando uma fonte de desinformação sobre certas pessoas, um exemplo emblemático é o caso do artigo do *wikipedia* que continha os dados sobre Jean Charles de Menezes, brasileiro morto pela polícia britânica em 2005 ao ser confundido com um terrorista em uma estação de metrô. As informações foram adulteradas para passar uma má impressão que relativizasse a ação policial, descobriu-se em investigação que alterações teriam sido feitas por meio de computador do governo britânico[11].

O problema atual de se utilizar o *fictious entry* é a citação dessas informações em outros meios de comunicação, que, em cadeia, torna muito difícil a contestação da informação.

---

[9] AMARAL, Adriana; COIMBRA, Michele. Expressões de ódio nos sites de redes sociais: o universo dos haters no caso #eunãomereçoserestuprada. Revista FAMECOS, Porto Alegre Contemporânea/comunicação e cultura, 2015.

[10] ALVES, F. B. ; CORREA, E. A. A. . op. cit.

[11] Governo teria alterado dados sobre Jean Charles na Wikipedia. EXAME. São Paulo, 07 de ago. 2014. Disponível em:<https://bityli.com/WQxJU>. Acesso em 03 jun. 2020.

2.1.3 Fake sciense

Fake Sciense consiste na adulteração ou fabricação de dados que dão embasamento a um estudo[12], geralmente possui a finalidade de dar visibilidade ao autor do estudo, com uma consequente ascensão em sua carreira. Essa modalidade ganhou grande repercussão na mídia brasileira em razão da discussão acerca do uso do medicamento hidroxicloroquina para o tratamento de pessoas acometidas pela COVID-19. No caso de um estudo em específico, houve o reconhecimento de erros de dados por parte do autor de um dos estudos que afirmava a eficácia do medicamento no tratamento de pacientes acometidos pelo vírus[13], não é possível saber se tais dados foram intencionalmente alterados pelo pesquisador, caso assim seja, esse seria um exemplo de *fake science*.

A consequência da proliferação dessa informação foi o uso, ou a indicação do uso, desse medicamento para tratar pacientes infectados pelo novo coronavírus em plena pandemia mundial, sem que efetivamente houvesse comprovação científica real de sua eficácia.

2.1.4 Fake profile

Os *fake profiles* são contas falsas criadas em redes sociais, ou mesmo em sites de notícias, para publicar sobre determinados assuntos ou para propagar notícias falsas ou gerar comentários massivos questionando a veracidade de alguma notícia[14]. As

[12] ALVES, F. B. ; CORREA, E. A. A. . op. cit

[13] AUTOR DE ESTUDO PRÓ-CLOROQUINA ADMITE ERROS EM PESQUISA. EXAME. São Paulo, 22 de mai. 2020. Disponível em : <encurtador.com.br/joGNY> Acesso em 02 jun. 2020.

[14] ALVES, F. B. ; CORREA, E. A. A. . op. cit

contas falsas são utilizadas para, por meio da forma lógica como se operam os algorítimos, gerar engajamento de algum setor da sociedade em prol de um movimento político ou de um agente político específico. Utiliza-se a denominada *hashtag* (#) para atacar ou exaltar algum político, ou algum assunto ligado a estes, a fim de ganhar visibilidade e atingir o engajamento do maior número de apoiadores.

Para este fim, têm-se utilizado os chamados bots, do inglês robôs, que seriam aparelhos eletrônicos com acesso à internet que se conectam a determinada rede social por meio de contas falsas, esses aparelhos são programados para replicar automaticamente as *hashtags* que beneficiem quem os programou, ou para gerar respostas automáticas àquelas que lhe são prejudiciais[15].

3 A QUESTÃO DA LIBERDADE DE EXPRESSÃO

Conforme exposto, a questão da propagação em massa de *fake news* traz inúmeros efeitos negativos para a sociedade. Por esta razão, há uma concentração de esforços na discussão sobre a criminalização das *fake news.* Tramitam no Congresso Nacional diversos projetos de lei que têm como objetivo tipificar a propagação intencional de notícias falsas. De mesmo modo, houve a criação de uma Comissão Parlamentar Mista de Inquérito para investigar a disseminação de notícias falsas contra adversários políticos do atual Presidente da República, Jair Bolsonaro, durante a campanha eleitoral do ano de 2019[16].

[15] BRANCO, Sérgio. Fake news e os caminhos para fora da bolha. Interesse Nacional, São Paulo, ano 10, n. 38 , p. 51-61, ago./out. 2017.

[16] CPMI-Fake News. Disponível em: <https://legis.senado.leg.br/comissoes/comissao?1&codcol=2292 > Acesso em: 02 jun. 2020.

Recentemente, o IBOPE realizou uma pesquisa que visou compreender qual a posição da população em relação à regulação das redes sociais a fim de se evitar a propagação de notícias falsas. O senso constatou que 90% da população consultada se demonstrou a favor da regulamentação da divulgação de informações em redes sociais[17]. A movimentação do Congresso Nacional, aliado ao apoio popular majoritário, desperta a preocupação com a forma com que será conduzido o processo de elaboração da lei, pois há grande preocupação com uma possível violação ao princípio constitucional da liberdade de expressão.

O artigo 5º, IV, prevê que é livre a manifestação do pensamento, sendo vedado o anonimato[18]. Este princípio, além de constituir elemento básico de liberdade individual, reforça a questão da liberdade de divulgação de informação por meio dos meios de comunicação. Corrobora com este princípio a Lei nº 12.965 de 23 de abril de 2014, conhecida como Marco Civil da Internet, que em seu artigo 3º, inciso I, reafirma a garantia da liberdade de expressão, comunicação e manifestação de pensamento nos meios digitais[19]. Por esta razão, a regulação da propagação de notícias via meios digitais pode gerar uma forma de censura, o que colidiria inevitavelmente com o princípio da liberdade de expressão.

Mais que isso, é importante também atentar-se ao fato de que o fortalecimento dos meios de comunicação também depende de canais independentes que possam contestar a veracidade ou

[17] 90% dos eleitores brasileiros apoiam regulamentação de redes sociais para combater 'fake news', diz pesquisa Ibope. G1, São Paulo, 02 de jun. de 2020. Disponível em:<encurtador.com.br/afuHT> Acesso em 02 jun. 2020.

[18] BRASIL. Constituição Federal, Brasília, 5 de outubro de 1988. Disponível em: <encurtador.com.br/dgpzI>. Acesso em: 02 jun. 2020.

[19] BRASIL. Lei nº 12.965, de 23 de abril de 2014. Disponível em: <encurtador.com.br/ksyU7>. Acesso em: 02 jun. 2020.

checar fatos divulgados em veículos oficiais de comunicação, caso contrário, há a possibilidade do domínio dos meios de notícia por uma parcela muito pequena de mídias. A popularização da divulgação de notícias, principalmente após o advento das redes sociais, apesar de facilitar a divulgação de notícias falsas, facilitou o trabalho de *fact checking* por mídias independentes ou até mesmo pelo próprio usuário, receptor da informação.

O temor das consequências da regulação da divulgação de notícias nos meios virtuais gera também atinge principalmente a classe dos jornalistas. Por este motivo, em palestra realizada no Tribunal Superior Eleitoral, em 16 de maio de 2019, o palestrante Ricardo Gutièrrez, Secretário-Geral da Federação Europeia de Jornalistas, afirmou a necessidade de unir esforços de diversos setores que influenciam na comunicação das pessoas, como as empresas Google, Facebook, Twitter, entre outras, e a academia, os jornalistas e a sociedade em geral, a fim de criar uma imunidade às *fake words*, fortalecendo o combate a desinformação e prezando pela qualidade da prestação de serviço pelos meios de comunicação responsáveis[20].

4 POSSIBILIDADE DO ENQUADRAMENTO DAS *FAKE WORDS* EM TIPO PENAL EXISTENTE

Não há dentro do ordenamento jurídico brasileiro uma tipificação penal da divulgação de notícias falsas, na verdade há mecanismos cíveis e penais que buscam coibir e punir a propagação. No entanto, não existe um critério preestabelecido que diferencie uma fraude civil de uma fraude penal, pois a

[20] Seminário Internacional Fake News e Eleições : anais. – Brasília : Tribunal Superior Eleitoral, 2019. p. 31.

valoração da intensidade desta varia de acordo com o sentimento político de cada época[21].

Portanto, inexistindo tipo penal específico, a divulgação intencional de notícias previamente sabidas como falsas poderia ser enquadrada em algum tipo penal já existente no ordenamento jurídico pátrio?

4.1 Estelionato

Estelionato é crime contra o patrimônio previsto no Código Penal Brasileiro[22]:

> 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.

Segundo o autor Cezar Roberto Bitencourt[23], pode ser praticado contra qualquer pessoa, seja jurídica ou física, e o bem jurídico tutelado é o patrimônio, ou seja, necessariamente deve haver lesão patrimonial para que delito seja consumado. Portanto, o autor deve agir com a intenção de ludibriar a vítima, obtendo dessa forma vantagem indevida. Entende-se que qualquer vantagem patrimonial pode ser objeto do crime de estelionato, seja coisa móvel, imóvel, direitos pertencentes à vítima, em resumo, qualquer vantagem que seja economicamente proveitoso.

---

[21] GRECO, Rogério. Curso de direito penal: parte geral - v. 2. 16. ed. Niterói: Impetus, 2015. p. 845.

[22] BRASIL. Código Penal. Rio de Janeiro, 7 de dezembro de 1940. Disponível em: <encurtador.com.br/BDOQY>. Acesso em: 02 jun. 2020.

[23] BITENCOURT, Roberto, C. Tratado de direito penal 3 - parte especial: crimes contra o patrimônio até crimes contra o sentimento religioso e contra o respeito aos mortos. São Paulo: Saraiva, 2018. . 9788553610426. Disponível em: <encurtador.com.br/oPTZ1>. Acesso em: 03 jun. 2020

No entanto, é difícil enquadrar a divulgação de *fake news* no tipo penal de estelionato, visto que, mesmo havendo a intenção do autor em divulgar os fatos falsos, a obtenção dos valores se dá em grande parte mediante *adsense* da empresa Google, que seria a responsável por direcionar os anúncios a serem exibidos em determinada página. Nesta lógica, é difícil se vislumbrar uma lesão patrimonial, visto que houve o recebimento de contraprestação pelos serviços de divulgação, da empresa anunciante em favor do Google, bem como houve a exibição do anúncio em veículo digital que permitiu a divulgação da marca. Portanto, o Google atua intermediando os anúncios, de acordo com o nicho que se pretende atingir. Do ponto de vista penal, não houve nenhuma violação que seja passível de responsabilização do divulgador das notícias, o que não o isenta de ser condenado à reparação por danos morais em uma eventual ação cível, a ser analisada caso a caso.

Ademais, houve, em 2019, inovação legislativa quanto ao crime de estelionato, trazida pela Lei nº 13.964[24], de 24 de dezembro de 2019. A referida lei tornou o estelionato um crime de ação penal pública condicionada à representação, salvo nos casos em que a vítima seja: a Administração Pública, direta ou indireta; criança ou adolescente; pessoa com deficiência mental; ou maior de 70 (setenta) anos ou incapaz.

Tal alteração tornaria a persecução penal do crime de estelionato ainda mais dificultoso nos casos que envolvam divulgação de notícias falsas em meio digital, pois nesse caso o Google seria a pessoa jurídica lesada, em razão de ser ela a responsável pelo pagamento pela hospedagem da propaganda no

[24] BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Disponível em: <ehttps://bityli.com/o5yeY>. Acesso em: 03 jun. 2020.

site (adsense). Deste modo, entende-se que o Google seria obrigado a representar uma denúncia junto ao Ministério Público para que fosse apurada a conduta criminosa[25].

Portanto, não parece ser possível considerar crime de estelionato a divulgação intencional de *fake words* em sites da internet e seria ainda mais difícil considerar crime de estelionato os casos que envolvam esse tipo de divulgação em redes sociais, tendo em vista a ausência da obtenção de vantagem patrimonial por meio de anúncios.

4.2 Crimes contra a honra

No ordenamento jurídico pátrio há a possibilidade da responsabilização penal do indivíduo que propaga intencionalmente notícias falsas, no entanto, condicionada à intenção do autor em causar lesão à honra da pessoa lesionada. Os crimes contra a honra estão previstos no Título; Capítulo V; do artigo 138 ao 145. Importante realizar a diferenciação dos tipos penais de crimes contra a honra, a fim de se determinar se a divulgação das notícias falsas violou ou não algum destes dispositivos penal. Nesses casos, para que se proceda a ação penal, é necessário que o ofendido ofereça a queixa-crime, em razão desses tipos penais serem de ação penal privada, conforme previsto no artigo 145 do Código Penal.

Conforme lição de Greco[26], a honra é algo que se constrói durante toda a vida do indivíduo, portanto, a possibilidade de uma mera acusação, mesmo que leviana ou infundada, destruir todo essa construção extrapola a esfera civil, sendo esta a

[25] TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. Curso de Direito Processual Penal. Salvador-BA: Juspodivm, 2019. p. 263.
[26] GRECO, Rogério. op. cit.

argumentação central para a importância de se enquadrar a lesão à honra como um ilícito penal, que pode ser de três formas: calúnia, difamação e injúria.

4.2.1 Calúnia

A calúnia consiste na acusação falsa de que alguém cometeu fato criminoso. Segundo Nucci [27] a calúnia seria uma difamação qualificada, portanto, uma espécie de difamação, atingindo a honra objetiva da pessoa. O tipo penal está previsto no art. 138, mas seu parágrafo primeiro estende o tipo penal àquela pessoa que propalar ou divulgar a calúnia divulgada por outra pessoa.

Nesse sentido, a propagação de *fake words*, de qualquer das espécies, que imputem falsamente um crime a alguém preenche os requisitos necessário para a configuração do crime de calúnia, estendendo-se suas consequências àqueles que continuarem a replicar o fato sem constatar sua veracidade.

4.2.2 Difamação

Quanto ao crime de difamação, consuma-se o fato típico quando o autor imputa fato ofensivo a outrem. A diferença entre este tipo penal e a calúnia é o fato que se atribui à vítima, que no caso da difamação não se trata de fato criminoso, mas sim desabonador à honra[28].

[27] Souza, N.G. D. Curso de Direito Penal - Parte Especial - Vol. 2, 3ª edição. Grupo GEN, 10/2018. 9788530982973. Disponível em: <encurtador.com.br/enN37>. Accesso em: 02 Jun 2020

[28] BITENCOURT, Roberto, C. Tratado de direito penal 2 - parte especial: crimes contra a pessoa. Editora Saraiva, 2019. 9788553611591. Disponível em: <encurtador.com.br/jrstV>. Accesso em: 02 Jun 2020

Portanto, a publicação falsa de notícias desabonadoras à honra de alguém, seja essa pessoa jurídica ou física, pode dar causa a uma queixa-crime de difamação, caso alguma pessoa sinta que tenha tido sua honra ofendida pela notícia propagada.

4.2.3 Injúria

Quanto ao crime de injúria, configura-se quando há a atribuição de atributos pejorativos ao ofendido, e não de fatos. Importante ressaltar que no caso de imputação de conduta prevista como contravenção penal o fato é enquadrado como injúria, sendo calúnia apenas a imputação falsa de conduta prevista como crime[29].

Por consequente, há possibilidade de se responsabilizar penalmente, pelo crime de injúria, pessoa que se utiliza da propagação de qualquer das modalidades de *fake words* para ofender alguém, desde que o ofendido ofereça a queixa-crime, como previsto legalmente.

5 CONCLUSÃO

Ponderando os fatores que influenciam diretamente na questão da propagação de *fake words*, percebe-se que muitos fatores influem diretamente na questão. No entanto, dentre todos os pontos de reflexão que o assunto demanda, há de se ter especial cuidado quanto a preservação do direito constitucional de livre manifestação de pensamento.

Uma regulação que se aplique especificamente à divulgação de notícias ou informações pelos meios digitais pode gerar uma violação ao direito de liberdade de expressão das pessoas. Em um

[29] GRECO, Rogério. op. cit.

momento em que há uma polarização preocupante da política brasileira, deve-se tratar a questão da liberdade como tema central das decisões acerca deste tipo de regulação. Importante também a reflexão de Norberto Bobbio acerca da questão da tolerância, tema intimamente ligada à liberdade. O cerceamento da liberdade costuma ser ainda mais gravoso em relação às parcelas da sociedade que já sofrem tem direitos tolhidos, ditas minorias[30].

Desta forma, havendo possibilidades de se punir os responsáveis por propagar maliciosamente fatos inverídicos, com a intenção de prejudicar pessoas ou setores da sociedade, seja na esfera penal, eleitoral ou cível, o ideal é que se preserve o direito à livre manifestação das pessoas. Dessa forma, pune-se os excessos derivados deste direito, ao passo que se preserva um direito que é um dos pilares para a manutenção do Estado Democrático de Direito. Ademais, é necessário que haja um fortalecimento da mídia de forma geral, a fim de fortalecer a qualidade da informação prestada pelos veículos de informação, incentivando as pessoas a consumirem notícias de fontes confiáveis, não sendo proporcional a criminalização da questão da divulgação de *fake words*[31].

REFERÊNCIAS

OLIVEIRA, André Soares; GOMES, Patrícia Oliveira. OS LIMITES DA LIBERDADE DE EXPRESSÃO: FAKE NEWS COMO AMEAÇA A DEMOCRACIA. R. Dir. Gar. Fund., Vitória, v. 20, n. 2, p. 93-118, maio/agosto, 2019

BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Resolução nº 23.610, de 18 de dezembro de 2019. Disponível em: <https://bityli.com/Itp81 >.

[30] BOBBIO, Norberto. A Era dos Direitos. Rio de Janeiro: Campus. 1996.

[31] BRANCO, Sérgio. Fake news e os caminhos para fora da bolha. Interesse Nacional, São Paulo, ano 10, n. 38 , p. 51-61, ago./out. 2017.

Tandoc, Edson & Lim, Zheng & Ling, Rich. (2017). Defining "Fake News": A typology of scholarly definitions. Digital Journalism. 1-17. 10.1080/21670811.2017.1360143. Disponível em:<https://bityli.com/tsb2R >.

ALVES, F. B.; CORREA, E. A. A. Análise das redes de relações sociais e o controle jurídico de fake words. In: Fabrício Polido, Lucas Anjos e Luíza Brandão. (Org.). Políticas, internet e sociedade. 1ed.Belo Horizonte: IRIS, 2019, v. 1, p. 158-169.

SOBRAL, Cristiano. A responsabilidade civil dos provedores e de terceiros pelas fake News. Disponível em: <encurtador.com.br/BLYZ6>. Acesso em: 02 jun. 2020.

Adsense do Google. Disponível em: <https://www.google.com.br/adsense/start/>

AMARAL, Adriana; COIMBRA, Michele. Expressões de ódio nos sites de redes sociais: o universo dos haters no caso #eunãomereçoserestuprada. Revista FAMECOS, Porto Alegre Contemporânea/comunicação e cultura, 2015.

Governo teria alterado dados sobre Jean Charles na Wikipedia. EXAME. São Paulo, 07 de ago. 2014. Disponível em:<https://bityli.com/WQxJU>.

AUTOR DE ESTUDO PRÓ-CLOROQUINA ADMITE ERROS EM PESQUISA. EXAME. São Paulo, 22 de mai. 2020. Disponível em : <encurtador.com.br/joGNY>

BRANCO, Sérgio. Fake news e os caminhos para fora da bolha. Interesse Nacional, São Paulo, ano 10, n. 38 , p. 51-61, ago./out. 2017.

CPMI-Fake News. Disponível em: <https://legis.senado.leg.br/comissoes/comissao?1&codcol=2292 >

90% dos eleitores brasileiros apoiam regulamentação de redes sociais para combater 'fake news', diz pesquisa Ibope. G1, São Paulo, 02 de jun. de 2020. Disponível em:<encurtador.com.br/afuHT> Acesso em 02 jun. 2020.

BRASIL. Constituição Federal, .Brasília, 5 de outubro de 1988. Disponível em: <encurtador.com.br/dgpzI>

BRASIL.. Lei nº 12.965, de 23 de abril de 2014. Disponível em: <encurtador.com.br/ksyU7>.

Seminário Internacional Fake News e Eleições : anais. – Brasília : Tribunal Superior Eleitoral, 2019. p. 31.

GRECO, Rogério. Curso de direito penal: parte geral - v. 2. 16. ed. Niterói: Impetus, 2015. 845 p.

BRASIL. Código Penal. Rio de Janeiro, 7 de dezembro de 1940. Disponível em: <encurtador.com.br/BDOQY>.

BITENCOURT, Roberto, C. Tratado de direito penal 3 - parte especial: crimes contra o patrimônio até crimes contra o sentimento religioso e contra o respeito aos mortos. São Paulo: Saraiva, 2018. . 9788553610426. Disponível em: <encurtador.com.br/oPTZ1>.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Disponível em: <ehttps://bityli.com/o5yeY>.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. Curso de Direito Processual Penal. Salvador-BA: Juspodivm, 2019. p. 263.

BOBBIO, Norberto. A Era dos Direitos. Rio de Janeiro: Campus. 1996.

O PAPEL DO SUPREMO TRIBUNAL FEDERAL NA DEFESA DA PLURALIDADE DE IDEIAS EM TEMPOS DE DES(INFORMAÇÃO) E A SUA ATUAÇÃO PROATIVA NO

Daniele Aparecido Lopes Ribeiro[1]

RESUMO

O presente trabalho tem por finalidade discorrer sobre a relevância da livre manifestação de ideias em um Estado Democrático de Direito, destacando que as ditas fake news são incompatíveis com os ideais de liberdade de expressão. Ademais, discorre pontualmente sobre a investigação perpetrada pelo STF na defesa de suas prerrogativas constitucionais, posicionando-se pela constitucionalidade das medidas tomadas no bojo do presente procedimento administrativo.

Palavras-chave: Liberdade. Democracia. STF. *Fake news*.

ABSTRACT

This paper aims to discuss the relevance of the free expression of ideas in a Democratic State of Law, highlighting that the so-called fake news are incompatible with the ideals of freedom of expression. Furthermore, it punctually discusses the investigation carried out by the STF in defense of its constitutional prerogatives, positioning itself for the constitutionality of the measures taken within the scope of this administrative procedure.

Keywords: Freedom. Democracy. STF. Fake news.

[1] Advogado atuante na área de Direito Público. Bacharel em Direito pelo Centro Universitário de Brasília - UniCEUB. Aluno da pós-graduação lato sensu do Instituto Ceub de Pesquisa e Desenvolvimento – UniCEUB/ICPD.

1 INTRODUÇÃO

A primeira parte trata sobre a relevância do pluralismo de ideias em um Estado Democrático de Direito. Expressa os direitos fundamentais, como o da livre manifestação de pensamento, de expressão, de reunião, de informação, previstos em tratados internacionais, bem como positivados na CRFB/88. Narram-se, em apertada síntese, os reflexos da Ditadura Militar de 1964 na Constituição Federal de 1988, o que fez com que o Constituinte Originário indicasse no rol de direitos fundamentais individuais as liberdades, sendo estas cláusulas pétreas.

No tópico II, discute-se o tema da (des)informação – *fake news* – na atualidade, e suas implicações no contexto social e político. Para tanto, sem querer esgotar o tema, foram realizados breves comentários à obra 1984 de George Orwell, relacionando-a aos tempos atuais.

No tópico III, buscou-se destacar os principais aspectos discutidos no âmbito do Inquérito Policial n. 4.781, em que se discute a legitimidade ou não do Supremo Tribunal Federal na sua atuação proativa na investigação.

Em decorrência do tópico anterior, o tópico IV trata da necessária defesa ao Supremo Tribunal Federal, por entender que este age em consonância com os ditames constitucionais e infraconstitucionais, tendo papel crucial da defesa do Poder Judiciário – do próprio STF e de seus ministros.

2 PLURALISMO DE IDEIAS NA CONSTITUIÇÃO FEDERAL DE 1988

> "E eu digo não. E eu digo não ao não. É proibido proibir. É proibido proibir..."

É proibido proibir, Caetano Veloso, 1968.

A Constituição da República Federativa do Brasil de 1988[2] – CRFB/88 – preceitua em seu art. 5-IV que "é livre a manifestação do pensamento, sendo vedado o anonimato", bem como em seu inciso IX de que "é livre expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença". Trata-se de direito fundamental individual, não sendo possível a sua alteração sequer por emenda constitucional, por força do que disponhe o art. 60, § 4-IV, da CRFB/88.

Há destacar que tais direitos não se tratam de inovação da CRFB/88; mencionados postulados foram inspirados na Declaração Universal dos Direitos do Homem e do Cidadão[3] (1789), artigos 10 e 11, na Declaração Universal dos Direitos Humanos[4] (1948), em seus artigos 18 a 20, na Convenção Americana de Direitos Humanos[5] (1969) –, em seus artigos 12 a 16.

Mas não só.

Mister destacar que o Constituinte Originário[6], quando da discussão em Assembleia Constituinte dos direitos que seriam positivados como constitucionais na nova Carta Magna, levou em consideração o contexto histórico pelo qual o Brasil há pouco vivenciara, a Ditadura Militar de 1964 que perdurou até o ano de

[2] BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://tinyurl.com/czskwlw. Acesso em 01/06/2020.
[3] **Declaração dos Direitos do Homem e do Cidadão de 1789**. Disponível em: https://tinyurl.com/k96tkbt. Acesso em 01/06/2020.
[4] **Declaração Universal dos Direitos Humanos.** Disponível em: https://tinyurl.com/ycnawact. Acesso em 01/06/2020.
[5] **Convenção Americana de Direitos Humanos**. Disponível em: https://tinyurl.com/yclqj585. Acesso em 01/06/2020.
[6] BRASIL. **Emenda Constitucional n. 26**. Convoca Assembleia Nacional Constituinte e dá outras providências. Disponível em: https://tinyurl.com/ybvhpzj7. Acesso em 01/06/2020.

1985 – considerado, em verdade, golpe à democracia e atentado aos direitos fundamentais.

Naqueles tempos sombrios, o direito à liberdade de expressão foi um dos mais vilipendiados e combatidos por aqueles que detinham o poder: calaram-se a liberdade, a expressão do pensamento, a manifestação política e filosófica, o ser, o sentir, o viver. Como bem lembra Marcelo Torrelly[7] ao citar os dados oficiais da Comissão Nacional da Verdade de 2014, tem-se pelo menos a morte e o desaparecimento de 434 (quatrocentos e trinta e quatro) pessoas, além de 9 (nove) mil indígenas que foram dizimados pela repressão.

Não por outra razão, a Corte Interamericana de Direitos Humanos – CIDH – foi incitada a se manifestar sobre as violações aos direitos ocorridos no período da Ditadura Militar de 1964, no caso *Gomes Lund vs. Brasil*, (11/2010), oportunidade em que a mencionada Corte reconheceu as diversas violações sistemáticas aos direitos fundamentais, determinando uma série de medidas que deveriam ser adotadas pelo Brasil[8].

Bem como, o caso *Herzog e outros vs. Brasil* [9] (07/2018), em que a CIDH condenou o Brasil por violação ao Pacto de São José da Costa Rica, considerando a morte do jornalista Herzog como crime contra a humanidade, a despeito da previsão

[7] PIOVESAN, Flávia e outros, Impacto das Decisões da Corte Interamericana de Direitos Humanos na Jurisprudência do STF. Salvador: Ed. JusPodivm, 2020, p. 526.
[8] Idem, p.525/560.
[9] Corte Interamericana de Direitos Humanos. **Caso Herzog e outros vs. Brasil**. Sentença de 15/03/2018. Disponível em: https://tinyurl.com/y8zkmqjf. Acesso em 01/06/2020.

infraconstitucional do Brasil intitulada Lei de Anistia[10] (Lei 6.683/1979), considerada constitucional pelo STF na ADPF 153[11].

Vê-se, portanto, que a CRFB/88 cuidou de elevar a liberdade – e todas as suas formas e meios de manifestação lícitas – ao patamar de princípio fundamental do Estado Democrático de Direito, pautado na dignidade da pessoa humana. Além disso, cuidou de legitimar o Supremo Tribunal Federal – STF – como Corte Constitucional apta à defesa dos seus preceitos.

Não por outra razão o STF tem assumido importante papel na defesa do direito à liberdade de expressão e de pensamento. Tem-se como notórios alguns de seus julgados mais emblemáticos: a ADPF 130, ADI 4815, ADPF 187, ADPF 548, entre outras tantas.

A Ação de Descumprimento de Preceito Fundamental – ADPF – 130[12], julgada em 2009, sob a relatoria do Ministro Carlos Ayres Britto, a Lei de Imprensa (Lei 5.250/1967) foi declarada incompatível com a CRFB/88, por não estar em harmonia com os preceitos constitucionais de liberdade de imprensa, de pensamento e de expressão.

Em seu voto, o relator destacou que a imprensa livre é verdadeira irmã siamesa da democracia, salientando que a atuação da imprensa exerce verdadeiro mecanismo de defesa dos direitos à liberdade de pensamento e de expressão dos indivíduos, sendo que tais direitos são:

> [...] **liberdades que não podem arredar pé ou sofrer antecipado controle nem mesmo por força do Direito-lei**, compreensivo este das

[10] BRASIL. **Lei n. 6.683/1979**. Disponível em: https://tinyurl.com/y9uqlgga. Acesso em 01/06/2020.
[11] BRASIL. Supremo Tribunal Federal. **ADPF 153**. Disponível em: https://tinyurl.com/yaghnydg. Acesso em 01/06/2020.
[12] BRASIL. Supremo Tribunal Federal. **ADPF 130**. Disponível em: https://tinyurl.com/y7d9vjhw. Acesso em 02/06/2020.

> próprias emendas à Constituição, frise-se. Mas ainda, liberdades reforçadamente protegidas se exercitadas como atividade profissional ou habitualmente jornalística e coo atuação de qualquer dos órgãos de comunicação social ou de imprensa (**Grifo do autor**).

Nesta senda, o Ministro Menezes Direito defendeu que "não existe lugar para sacrificar a liberdade de expressão no plano das instituições que regem a vida das sociedades democráticas", além de que "quando se tem um conflito possível entre a liberdade e sua restrição deve-se defender a liberdade. O preço do silêncio para a saúde institucional dos povos é muito mais alto do que o preço da livre circulação das ideias".

Outro importante julgado da Corte Constitucional foi a Ação Direta de Inconstitucionalidade[13] – ADI – 4815, que tratou das biografias não autorizadas, no ano de 2015, sob a relatoria da Ministra Cármen Lúcia. Utilizou-se a técnica da interpretação conforme a Constituição para uma nova leitura constitucional dos artigos 20 e 21 do Código Civil, declarando-se inexigível a autorização prévia para a publicação de biografias para, deste modo, privilegiar "os direitos fundamentais à liberdade de expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença de pessoa biografada, relativamente a obras biográficas literárias ou audiovisuais".

Outro caso em que a Corte assumiu posição contramajoritária na defesa das liberdades de pensamento, reunião e de expressão, foi na ADPF 187[14], conhecida como Marcha da Maconha, no ano de 2011, sob a relatoria do Ministro

[13] BRASIL. Supremo Tribunal Federal. **ADI 4815**. Disponível em: https://tinyurl.com/ycdnuks2. Acesso em 02/06/2020.
[14] BRASIL. Supremo Tribunal Federal. **ADPF 187**. Disponível em: https://tinyurl.com/ycd39gkn. Acesso em 02/06/2020.

Celso de Mello. Em decisão unânime, a Corte assentou ser constitucional a marcha pacífica em defesa da legalização do uso da *cannabis*, dando interpretação conforme a Constituição ao art. 287 do Código Penal.

Para o relator, a marcha da maconha trata-se em verdade de um movimento social espontâneo e legítimo que reivindica, por meio da livre manifestação do pensamento, "a possibilidade da discussão democrática do modelo proibicionista (do consumo de drogas) e dos efeitos que (esse modelo) produziu em termos de incremento da violência".

Não há esquecer a ADPF 548[15], ano de 2018, sob a relatoria da Ministra Cármen Lúcia, que assegurou o pluralismo de ideias nas universidades, entendendo não ser constitucional a restrição da liberdade de pensamento e expressão sob o argumento da vedação da veiculação de propaganda eleitoral em prédios e outros bens públicos, ao teor do artigo 37 da Lei 9.504/1997.

Para a relatora, *"a única força legitimada a invadir uma universidade é a das ideias livres e plurais"*. Neste passo, o Ministro Celso de Mello acrescentou:

> Todos sabemos que **não há pessoas nem sociedades livres sem liberdade de expressão, de comunicação, de informação**, mostrando-se inaceitável qualquer deliberação estatal, seja ela executiva, legislativa ou judicial, cuja execução importe em controle do pensamento crítico, com o consequente comprometimento da ordem democrática (friso nosso).

Note-se que em todos estes julgados – entre tantos outros igualmente importantes –, a Corte Constitucional assume papel crucial na defesa das liberdades – de pensamento, expressão,

[15] BRASIL. Supremo Tribunal Federal. **ADPF 548**. Disponível em: https://tinyurl.com/yaw75wse. Acesso em 02/06/2020.

comunicação, informação, associação, reunião –, uma vez que o Estado Democrático de Direito tem por valor primaz a liberdade.

Tem-se, portanto, a liberdade como pilar da democracia, direito fundamental eleito pela CRFB/88 como princípio fundamental pautado na dignidade da pessoa humana, devendo ser defendido por todos os Poderes – Executivo, Legislativo e Judiciário – pelas instituições essenciais à justiça – Ministério Público, Advocacia pública e privada e Defensoria Pública –, bem como por toda a sociedade.

Feitas estas breves considerações sobre a importância do pluralismo de ideias em um Estado Democrático de Direito, bem como a sua defesa pelo STF, passa-se a discutir a seguir, o inquérito aberto pela Corte Constitucional para tratar sobre as Fake News.

3 A ERA DA (DES)INFORMAÇÃO NO SEU CONTEXTO SOCIAL E POLÍTICO – O FENÔMENO DAS *FAKE NEWS*

> "Guerra é paz; liberdade é escravidão; ignorância é força".
>
> Livro 1984, George Orwell, publicado em 1949[16]. Lema do Partido Interno.

A obra de George Orwell, intitulada 1984, nunca foi tão atual. Neste livro distópico, seu autor narra as mazelas oriundas de um Estado totalitário, em que a verdade é suprimida e alterada repetidas vezes para beneficiar seus próprios governantes. Aqui, a inveridicidade torna-se verdade incontestável.

O livro narra a tirania de um partido denominado Partido Interno, que altera os fatos do passado editando novas publicações com inverdades para benefício próprio. Assim, manipula-se a

[16] ORWELL, George. **1984**. Publicado em 1949, Editora Companhia das Letras.

sociedade da Oceânia (lugar onde se passa a história) para se perpetuarem no poder os seus tiranos.

Não bastasse isso, instala-se o Ministério da Verdade – responsável por alterar a verdade de acordo com as diretrizes do partido – e, para sua defesa, institui-se a Polícia do Pensamento como o departamento responsável por zelar e fazer valer as regras do partido totalitarista, perseguindo e aniquilando qualquer outro que tenha posição diversa daquela estabelecida pelo partido.

A perseguição à liberdade de expressão e de pensamento ia além disso. O partido estimulava os próprios cidadãos a denunciar qualquer vizinho, amigo ou familiar que tivesse manifestação político-partidária diferente daquela propagada pelo partido; além disso, havia equipamentos eletrônicos que sobrevoavam a cidade, sendo capazes de captar qualquer comportamento ou discurso contrário ao interesses do partido e, mesmo dentro de suas próprias residências, o Estado também instalava equipamentos de vigilância.

Apesar da obra ter sido publicada em 1949, ela se mostra presente na atualidade. As chamadas *Fake News*, ou notícias falsas, nada mais são do que a manipulação da verdade: no contexto social-político, busca-se alterar a realidade dos fatos para que se faça prevalecer um posicionamento político-partidário único, em que qualquer posição diversa deve ser motivo de rechaça.

Não há espaço para o pluralismo de ideias. Só há uma verdade; logo, não há democracia.

Veja que tal tema foi discutido na ADPF 548 – discutida no tópico anterior – em que o Ministro Luís Roberto Barroso destacou

que *"pensamento único é para ditadores e a verdade absoluta é própria das tiranias"*.

O livro demonstra os riscos à democracia e aos direitos fundamentais quando o fenômeno das *Fake News* não é devidamente combatido.

Com a revolução digital – oriunda com o advento da *internet* e dos meios eletrônicos – o comportamento da sociedade, no seu modo de buscar as informações, gradativamente foi sendo alterado. Constata-se, por exemplo, que os canais de informação antes eleitos pela sociedade, como os jornais, as revistas e a televisão, foram perdendo espaço; com o surgimento da *internet*, vieram as páginas – *sites* – de notícias; e, mais recentemente, as mídias sociais – *Facebook*, *Instagram*, *Twitter*, *WhatsApp*, *Telegram* e outros – que oferecem informações curtas e de fácil acesso.

É de bom tom lembrar que a doutrina menciona que os direitos fundamentais de quarta geração englobam o direito à democracia, à informação e ao pluralismo; os de quinta geração, conforme Augusto Zimmermann, são os direitos inerentes à realidade virtual, compreendendo o desenvolvimento da internet[17].

Vê-se, portanto, que os direitos fundamentais de quarta e quinta geração estão umbilicalmente "conectados", um soma-se ao outro, possibilitando o pluralismo de ideias e a promoção do Estado Democrático de Direito.

Todavia, as *Fake News* vão na contramão dos direitos acima citados, pois o que se busca é lançar a pós-verdade e a desinformação, culminando na divisão, na intimidação e no medo.

[17] LIMA, Larissa Pinho de Alencar. **Acesso à comunicação virtual é um direito fundamental**. Conjur. 09/07/2012. Disponível em: https://tinyurl.com/yaacxomz. Acesso em 02/06/2020.

A despeito das chamadas falsas notícias estarem presentes desde os tempos mais remotos[18], fato é que estas, associadas à rápida propagação pelos canais da *internet*, trazem consequências em uma maior extensão, uma vez que propositadamente tenta-se ludibriar a opinião pública, buscando-se, mais das vezes, alterar o curso político e social de uma nação e desestabilizar a democracia.

No contexto político brasileiro atual, o Tribunal Superior Eleitoral – TSE – tem assumido importante papel na defesa da democracia, a fim de combater a desinformação nas eleições. Neste rumo, para resguardar as eleições municipais no ano de 2020, o TSE, em 19/12/2019, aprovou uma série de resoluções, entre elas, a Resolução n. 23.610/2019[19], que trata especificamente no seu art. 9º, da responsabilidade dos partidos e candidatos de garantir a veracidade e a fidedignidade das informações, assegurando-se o direito de resposta e à indenização.

Na mesma resolução, tem-se, em seus artigos 27 a 41, dispositivos que tratam precipuamente da propaganda eleitoral na internet. Tratam, em apertada síntese, da determinação de que candidatos e partidos políticos têm o dever de garantir a veracidade das informações veiculadas, inclusive aquelas manifestadas por terceiros; veda-se o uso de mecanismos como o de impulsionamento e disparo em massa de conteúdo – inclusive aqueles de cunho inverídicos, sendo-lhes imputado, além de sanções penais, pagamento de multa e pagamento de indenização àqueles que se sentirem prejudicados, garantindo a estes o direito de resposta. Além disso, trata sobre a responsabilidade dos provedores de *internet*, que deverão obedecer às requisições

[18] BURKHARDT, Joanna M. **History of Fake News**. Disponível em: https://tinyurl.com/yctqgv4a. Acesso em 05/06/2020.
[19] BRASIL. Tribunal Superior Eleitora. **Resolução n. 23.610/2019.** Disponível em: https://tinyurl.com/y8u3oh86. Acesso em 02/06/2020.

judiciais de dados e registros eletrônicos, sob pena de pagamento de multa.

No que concerne à seara social, a propagação das *Fake News*, neste contexto, pode propiciar um ambiente polarizado e dividido, em que há somente uma única (in)verdade para cada lado, sendo a do outro combatida e rechaçada. Esclarece-se que não se defende aqui que deva existir tão só um único posicionamento, ao revés, pois a democracia é justamente aquela em que há pluralidade de ideias.

O que não é aceitável é o posicionamento pautado em *Fake News* – se falso, não há falar em benesse à democracia – em que se busca desestabilizar os fundamentos do Estado Democrático de Direito e vilipendiar os direitos fundamentais, individuais e coletivos, assegurados na Constituição.

Ora, as *Fake News* são o lado contrário à livre manifestação do pensamento e da expressão, uma vez que aquela é proferida, mais das vezes, para denegrir o outro, ludibriar e enganar, mover a opinião pública contra pessoas, instituições e ideias determinadas, para benefício próprio ou de outrem.

Com efeito, o Poder Judiciário – precipuamente o STF – tem sido instado repetidas vezes a se manifestar sobre o tema. Conforme delineado no tópico 1, é possível verificar o posicionamento contramajoritário do STF na defesa dos direitos fundamentais, destacando-se aqueles concernentes às liberdades.

Sem liberdade não há democracia; Democracia é liberdade!

Não por outra razão, defende-se que o STF assume papel crucial no combate ao Ministério da Verdade – que na obra de George Orwell é o órgão responsável por alterar a verdade – e à

Polícia do Pensamento – departamento que cuida de perseguir e aniquilar a livre manifestação de pensamento e de expressão.

Entretanto, há quem alegue que o STF na realidade tem assumido papel de Supremocracia[20], invadindo competências dos demais Poderes: Executivo e Legislativo.

Mais recentemente (14/03/2019), com a abertura do Inquérito pelo próprio Supremo para apurar as notícias fraudulentas (*fake news*) e ameaças veiculadas na *internet* contra a própria Corte, seus membros e familiares, o STF tem sofrido duras críticas quanto à sua legitimidade para apurar e julgar estes fatos, dada a competência constitucional atribuída ao Ministério Público – MP – de promover a ação penal (CF, art. 121-I); além disso, critica-se que mencionado inquérito viola princípios constitucionais individuais, como aqueles defendidos tão ferozmente pela própria Corte: a livre manifestação de ideias, de pensamento e expressão, de informação e reunião.

Contudo, na inércia do Ministério Público Federal – MPF –, na figura do seu PGR e dos Poderes Executivo e Legislativo, quem defenderá o Supremo Tribunal Federal?

4 A APURAÇÃO DAS *FAKE NEWS* NO ÂMBITO NO INQUÉRITO 4781 NO STF

> "Filha do medo, a raiva é mãe da covardia".
>
> As caravanas, Chico Buarque, 2017.

No dia 14/03/2019, o Presidente do Supremo Tribunal Federal, Ministro Dias Toffoli, determinou, de ofício, por meio da Portaria GP 69/2019, a abertura de inquérito para apurar fatos e infrações relativos às notícias fraudulentas (fake news) e ameaças

[20] VIEIRA, Oscar Vilhena. **Supremocracia**. Revista DIREITO GV 8. Disponível em: https://tinyurl.com/y9f5fbct. Acesso em 01/06/2020.

veiculadas na *Internet*, contra a Suprema Corte, seus ministros e familiares. Na mesma oportunidade, o Presidente designou o Ministro Alexandre de Moraes para conduzir o feito.

O Presidente do STF ponderou que "não existe um Estado Democrático de Direito nem democracia sem um Judiciário independente e sem uma imprensa livre[21]", ressaltando o papel da Suprema Corte na defesa das liberdades, precipuamente a da imprensa livre.

O Inquérito Policial – IP – 4781[22], que tramita em sigilo, tem como fundamento os artigos 13-I e 43, *caput*, do Regimento Interno do Supremo Tribunal Federal[23] – RISTF. Transcreve-se:

> Art. 13. São atribuições do Presidente:
>
> I – velar pelas prerrogativas do Tribunal;
>
> [...]
>
> Art. 43. Ocorrendo infração à lei penal na sede ou dependência do Tribunal, o Presidente instaurará inquérito, se envolver autoridade ou pessoa sujeito à sua jurisdição, ou delegará esta atribuição a outro Ministro.
>
> Parágrafo Primeiro: **nos demais casos**, o Presidente poderá proceder na forma deste artigo **ou** requisitar a instauração de inquérito à autoridade competente (grifo nosso).

A então Procuradora-Geral da República, Raquel Dodge, promoveu o arquivamento do supracitado inquérito em 16/04/2010, alegando ser genérico o objeto da investigação, a ausência de informações sobre o IP, o deferimento de medidas cautelares sem prévia manifestação do MPF e a notícia de proibição de matéria jornalística, destacando ofensa ao devido processo legal

[21] BRASIL. Supremo Tribunal de Federal. Portal de notícias. Disponível em: https://tinyurl.com/ycz5py9q. Acesso em 02/06/2020.

[22] BRASIL. Supremo Tribunal Federal. Disponível em: https://tinyurl.com/ybzuxzc7. Supremo Tribunal. Acesso 02/06/2020.

[23] BRASIL. Regimento Interno do Supremo Tribunal Federal. Disponível em: https://tinyurl.com/gnmv7qq. Acesso em 02/06/2020.

– princípio da legalidade, do contraditório, da ampla defesa e da imparcialidade do juízo – e ao sistema penal acusatório (CF, art. 129-I)[24].

O Ministro Alexandre de Moraes, todavia, negou o arquivamento do IP por entender que o sistema acusatório não se estenderia às investigações penais, bem como o feito estar amparado pelo RISTF. Sobre o objeto do IP, destacou[25]:

> O objeto deste inquérito é clara e específico, consistente na investigação de notícias fraudulentas (*fake news*), falsas comunicações de crimes, denunciações caluniosas, ameaças e demais infrações revestidas de *animus caluniandi*, *diffamandi* ou *injuriandi*, que atinjam a honorabilidade institucional do Supremo Tribunal Federal e de seus membros, bem como a segurança destes e de seus familiares, quando houver relação com a dignidade dos Ministros, inclusive com a apuração do vazamento de informações e documentos sigilosos, com o intuito de atribuir e/ou insinuar a prática de atos ilícitos por membros da Suprema Corte, por parte daqueles que tem o dever legal de preservar o sigilo; e a verificação da existência de esquemas de financiamento e divulgação em massa nas redes sociais, com o intuito de lesar ou expor a perigo de lesão a independência do Poder Judiciário e ao Estado de Direito (grifo nosso).

Vê-se, portanto, que desde a abertura do mencionado inquérito, o feito tem sido conduzido exclusivamente pelo STF, sem qualquer participação do Ministério Público.

Na condução do inquérito, o ministro responsável proferiu decisão no dia 15/04/2019 determinando à Crusoé e ao O Antagonista a retirada de notícia que tratava sobre suposta notícia

[24] BRASIL. Ministério Público Federal. Disponível em: https://tinyurl.com/ybcbwvr4.Acesso em 02/06/2020.
[25] Disponível em: https://tinyurl.com/ycd9bkeh. Acesso em 02/06/2020.

inverídica sobre ministro do Supremo, sob a alegação de "claro abuso no conteúdo"[26].

Diante disso, o STF sofreu duras críticas da sociedade civil, jurídica e política, da imprensa e outros, por entenderem que tal medida configurava censura prévia e violação à liberdade de expressão e de informação, ofendendo os incisos V, X, XIV do art. 5, e o art. 220, p. 1, da CRFB/88. Após esclarecimentos da PGR e do MP-PR, o Ministro responsável restabeleceu a veiculação das matérias supostamente censuradas no dia 18/04/2019[27].

Mister destacar que, no âmbito do STF, foi protocolada a **ADPF 572**[28] em 23/03/2019 pelo Partido Rede Sustentabilidade, em face da Portaria GP n. 69/2019, que determinou a abertura do IP 4781; o Ministro Edson Fachin foi sorteado como relator do processo.

Em manifestação à referida ADPF, a Procuradoria-Geral da República, em 20/02/2020, manifestou-se sobre o feito, alegando, entre outras razões, que a "investigação preliminar conduzida pelo Supremo Tribunal Federal não pode ser realizada à revelia da atribuição constitucional do Ministério Público na fase pré-processual da persecução penal, havendo de ser observados os direitos e as garantias fundamentais dos sujeitos da apuração[29]".

[26] Migalhas, **Moraes manda Crusoé e O Antagonista retirarem do ar reportagem que cita Toffoli**. 15/04/2019. Disponível em: https://tinyurl.com/yaefpoau. Acesso em 02.06.2020

[27] BRASIL. Supremo Tribunal Federal. Portal de notícias. Disponível em: https://tinyurl.com/yanmrcjf. Acesso em 02/06/2020.

[28] BRASIL. Supremo Tribunal Federal. **ADPF 572**. Disponível em: https://tinyurl.com/ybgn5324. Acesso em 02.06.2020.

[29] BRASIL. Supremo Tribunal Federal. **Parecer da Procuradoria-Geral da República na ADPF 572**. Disponível em: https://tinyurl.com/ybmyrb9f. Acesso em: 02/06/2020.

O julgamento da mencionada ADPF será na data de 10/06/2020, conforme consta no sítio do Supremo Tribunal Federal.

Com efeito, no dia 27/05/2020, o Ministro Alexandre de Moraes autorizou diversas diligências no âmbito do IP 4781. Em sua decisão[30], esclareceu que, pelas provas obtidas, verificou-se a existência de uma associação criminosa cujo objetivo era a de disseminar notícias falsas sobre autoridades e instituições democráticas – sendo uma delas o próprio STF –, pautadas no discurso do ódio, subversão da ordem e incentivo à quebra da normalidade institucional.

E mais: elucidou que as investigações apontam para uma estrutura aparentemente financiada por empresários que contribuem com recursos dos mais variados tipos, além de promoverem o impulsionamento de notícias inverídicas e ofensivas por meio de publicações em redes sociais, que atingem milhares de pessoas, com o fito de desestabilizar as instituições democráticas e a independência dos poderes.

Feitas as diligências, aqueles que se sentiram de algum modo afetados pela medida de busca e apreensão determinada pela Corte, defenderam, entre outras razões, que a atuação do Supremo Tribunal Federal violava direitos fundamentais individuais, como o da livre manifestação do pensamento e da expressão.

[30] Brasil. Supremo Tribunal Federal. Decisão do Ministro Alexandre de Moraes no **Inquérito 4781**. Disponível em: https://tinyurl.com/ya86r79t. Acesso em 02/06/2020.

Destaca-se que na data de 01/06/2020, o Ministro Alexandre de Moraes autorizou aos investigados o pleno acesso aos autos do IP 4781[31].

Em apertada síntese, os argumentos trazidos pela PGR e pelo partido Rede Sustentabilidade sobre a eventual inconstitucionalidade do IP 4781 são: (1) ofensa ao sistema acusatório adotado pela CRFB/88; (2) ofensa ao princípio do devido processo legal; (3) ofensa ao princípio da imparcialidade do juízo – uma vez que a própria Corte investiga e julga; (4) ofensa ao princípio do juiz natural – pois a designação do Ministro Alexandre de Moraes foi feita diretamente, sem distribuição; (7) ofensa ao princípio da ampla defesa e do contraditório – haja vista o inquérito tramitar em sigilo; (6) a incompetência do STF em julgar os casos em que seus próprios Ministros figuram como vítimas; (7) a não previsibilidade no art. 43, RISTF, de que a investigação extrapola a sede do STF; (8) a não recepção do art. 43, RISTF; (9) ausência de justa causa – por não haver a referência a fatos concretos ou delimitação do seu objeto; (10) violação aos preceitos da liberdade de pensamento e expressão e da pluralidade de ideias em toda sua extensão.

Por outro lado, os argumentos favoráveis à constitucionalidade do inquérito promovido de ofício pelo próprio STF são: (1) há previsão expressa no RISTF da atribuição do Presidente do STF de zelar pelas prerrogativas do Tribunal; (2) o RISTF determina que, ocorrendo infração no âmbito do Tribunal, o Presidente instaurará inquérito, podendo delegar a outro Ministro; (3) que o sistema acusatório não se estenderia às investigações penais; (4) que os Ministros têm jurisdição em todo território

[31] BRASIL. Supremo Tribunal Federal. Portal de notícias. Disponível em: https://tinyurl.com/ycg7rjon. Acesso em 02.06.2020.

nacional (CF, art. 92, p.2), sendo que a infração contra eles cometida implica em ofensa ao próprio STF; (5) a competência do STF para defesa da Corte, de seus ministros e familiares; (5) que a investigação não ser exclusiva de um único órgão, como o Ministério Público ou a Polícia Judiciária; (6) a defesa das prerrogativas da Corte e de seus Ministros decorrem dos poderes implícitos; (7) sigilo do inquérito pautado no art. 20, caput, do CPP.

No tópico seguinte, tentar-se-á, de modo sucinto, demonstrar as razões pelas quais a atuação do Supremo Tribunal Federal, no inquérito 4781, mostra-se constitucional.

5 A NECESSÁRIA DEFESA DO STF E DE SUAS PRERROGATIVAS CONSTITUCIONAIS

> "Pai, afasta de mim esse cálice. Pai, afasta de mim esse cálice. Pai, afasta de mim esse cálice, de vinho tinto de sangue".
>
> Cálice, Chico Buarque, 1973.

Em artigo publicado no *site* JOTA, o autor Eugênio Pacelli[32] defende que "os ataques conscientemente mentirosos desferidos à Suprema Corte não traduzem exercício de liberdade de expressão". Ressalta:

> As chamadas *Fake News,* que triunfaram nas redes sociais, mas não só – quem sabe a mídia *oficial* reconheça seus pecados também? – são mentiras criadas a partir de um propósito: enganar seus interlocutores e atingir alvos previamente escolhidos. Isso nada tem que ver como liberdade de expressão (grifo nosso).

[32] PACELLI, Eugênio. **Em defesa do STF e dos Tribunais**. JOTA; 28/05/2020. Disponível em https://tinyurl.com/ybuzy2t5. Acesso em 03.06.2020.

Por outro lado, há que entenda que as chamadas "*fake news*" investigadas pelo STF na realidade tratam-se de opinião crítica lançada sobre seus ministros.

Entretanto, não é este o posicionamento defendido no presente trabalho. Na linha do que defende o professor Eugênio Pacelli – e conforme já posto no item III deste trabalho –, as *fake news* nada tem a ver com liberdade de expressão; ao revés, seu propósito, no contexto em comento, é desestabilizar a democracia, movendo a opinião pública contra a Instituição do Supremo Tribunal Federal e seus Ministros.

Liberdade de expressão não se coaduna com discurso de ódio; tampouco com debates eivados de "*desapego e desapreço pela própria ideia de democracia, e também do exercício da cidadania, por meio da distorção deliberada e consciente de fatos comuns ao senso comum*[33]".

Pois bem. De fato, a Constituição Federal atribui ao Ministério Público a titularidade da Ação Penal. Entretanto, a investigação penal não é atribuição exclusiva do Ministério Público, pois, como se sabe, a Polícia Judiciária também a faz.

De todo modo, pelo deslinde das investigações promovidas pela Corte no IP 4781, verifica-se que, de fato, são incontestáveis as provas que indicam a formação de uma organização criminosa que, livre e conscientemente, desferem *fake news* contra as Instituições democráticas, com o propósito de abalar os fundamentos do Estado Democrático de Direito.

Ora, percebe-se com isso que o *Parquet* quedou-se inerte na sua atribuição primordial de zelar pela ordem jurídica e pelo

[33] PACELLI, Eugênio. **Em defesa do STF e dos Tribunais**. JOTA. Disponível em https://tinyurl.com/ybuzy2t5. Acesso em 03.06.2020.

regime democrático (art. 127, *caput*, CRFB/88), pois, caso não fosse a atuação proativa do próprio Supremo em zelar pela prerrogativas institucionais da mais alta Corte e dos seus ministros, provavelmente o esquema criminoso exposto no inquérito continuaria na zona obscura dos crimes cibernéticos.

Corrobora para tal argumento, o fato de que antes de 14/03/2019 – data da Portaria GP 69/2019 que determinou a abertura do inquérito –, e mesmo depois, não há quaisquer diligências por parte da PGR a fim de investigar as *Fake News* contra a Corte Constitucional.

A Suprema Corte, um dos Poderes que atestam a existência de um Estado Democrático de Direito, não pode ficar à mercê da ineficiência do Ministério Público em zelar pela democracia e pelas suas instituições; mais ainda, não pode ficar cativo à escolha do *Parquet* de quando, ao seu bel-prazer, investigar, por razões outras inescusáveis.

Há lembrar que o jurista Eugênio Pacelli[34] destaca o art. 5, LIX, da CF, bem como o art. 29, do CPP, quem possibilitam a ação privada nos crimes de ação pública, se esta não for promovida no prazo legal pelo *Parquet*.

Ora, *data venia* aos que pensam de modo contrário, estar-se-ia criando um Leviatã sobremaneira poderoso, qual seja: aquele que ocupa a posição de PGR – sendo este indicado pelo Presidente da República, nomeado após aprovação do Senado Federal, com mandato de 2 (dois) anos, podendo ser reconduzido sucessivas vezes. Diferente dos Ministros da Suprema Corte que, após passarem pelo mesmo rito, ao assumirem a função de ministros da

[34] PACELLI, Eugênio. **Em defesa do STF e dos Tribunais**. JOTA. Disponível em https://tinyurl.com/ybuzy2t5. Acesso em 03.06.2020.

alta Corte, possuem a garantia da vitaliciedade do cargo, perdendo a função somente após processo de *impeachment*.

Não seria razoável, sequer constitucional, dotar à PGR a legitimidade única e exclusiva para defesa do Poder Judiciário, precipuamente quando decide, por quaisquer razões que seja, ficar inerte, quando há claras evidências de ataques sistemáticos à Corte.

Há destacar que a CRFB/88, art. 34-VII, "a" e "b", que trata dos princípios constitucionais sensíveis, atribui ao *Parquet* um dever-ser, isto é, o dever de intervir nos casos necessários para assegurar a observância da forma republicana, do sistema representativo e do **regime democrático**; além da imposição de intervir na defesa da dignidade da pessoa humana, devendo representar ao STF (CRFB/88, art. 36-III).

É por esta razão que o RISTF, prevê, em seu artigo 43, a possibilidade de abertura de inquérito de ofício pelo Presidente do STF, podendo este delegar a quem quiser dentre seus os ministros para conduzir o feito. E mais: em seu parágrafo primeiro, assevera a possibilidade de se estender a investigação inclusive fora das dependências da sede do Supremo, ficando a critério da própria Corte requisitar ou não a abertura do inquérito a outro órgão competente.

Há dizer que o RISTF foi recepcionado pela Constituição Federal com status de lei ordinária e não há declaração de inconstitucionalidade de seus preceitos aqui elencados.

Com efeito, conforme artigo publicado no Consultor Jurídico – Conjur – de autoria do jurista Lênio Streck[35], há destacar que o Presidente do STF, em uma interpretação extensiva, entendeu que quando os crimes perpetrados atingem todos os seus ministros, a competência será do STF. Dando razão a esta justificativa, defende o jurista:

> Tal fato tem a sua razão de ser em dois pontos: em primeiro lugar, há um caso explícito de atentado à própria jurisdição do STF (e isso atinge os princípios da democracia e da República), fazendo com que o próprio STF deva eliminar o *contempt of court*; em segundo, em um ambiente virtual, a velha noção de um local físico não faz mais sentido, embora o próprio § 1 do art. 43, do RISTF, autorize o Presidente do Tribunal agir de acordo com o disposto no caput do mesmo artigo, mesmo quando a infração não se dê nas dependências físicas do STF. Ainda há um terceiro elemento: o STF e a PGR. Por isso o RISTF se apresenta como um remédio nas hipóteses nas quais quem deveria defender o STF de um contempt of court não o faz. No caso, até se coloca contra o STF (em movimento na contração do que havia feito antes – basta ver a manifestação do dia 27/05/2020 da lavra de Aras).

Lembra o autor que o STF, em outro momento, também instaurou inquérito de ofício, no âmbito do HC 152.720, para investigar abuso na utilização de algemas em Sérgio Cabral. Veja que, nesta oportunidade, o Ministério Público não se opôs à legitimidade da Corte em instaurar o inquérito de ofício.

E mais: conforme aponta o jurista, o argumento de quebra de imparcialidade também não se sustenta – os juízes são investigados e julgados pelos próprios Tribunais que conduzem a investigação.

[35] STRECK, Lênio. **Inquérito judicial do STF: o MP como parte ou "juiz das garantias"?.** Conjur. 28/05/2020. Disponível em: https://tinyurl.com/y9vmupdu. Acesso em 03/06/2020.

Destaca, ainda, a incoerência advinda da PGR, uma vez que em 10/2019 apoiou-se o inquérito conduzido pelo STF, sendo as palavras do Procurador-Geral da República, Augusto Aras: "O Ministro Toffoli exerceu regularmente as atribuições que lhe foram concedidas pelo RISTF"; todavia, mais recentemente o contesta. Além do mais, frisa o jurista:

> De pronto, a propósito, é bom lembrar que, em sendo a insurgência contra o STF vida em maior grau do PGR, só aí já se contata, de há muito, uma omissão do órgão, que, ao que parece, vem praticando uma adesão seletiva ao sistema acusatório e um garantismo *ad hoc*.

De mais a mais, o autor pontua que o artigo 242 do Código de Processo Penal prevê, expressamente, a busca e apreensão de ofício pelo juiz e que mencionado artigo vigora no ordenamento jurídico; bem como, a abertura de inquérito de ofício nos moldes o art. 5-I, do CPP.

Por último, sustenta que tal posicionamento aguerrido da PGR mais lembra a de um "juiz das garantias", uma vez que se tem defendido a exclusividade do Ministério Público na condução, inclusive, da investigação preliminar.

Por todas estas razões, entende-se que a abertura do inquérito de ofício pelo Supremo Tribunal Federal encontra guarida constitucional, quando traduz-se na defesa Poder Judiciário – sobretudo o STF e seus ministros –, uma vez que figura um dos fundamentos de um Estado Democrático de Direito e que, sem um Judiciário independente, não há democracia, como bem salientou o Presidente da Corte na abertura do mencionado inquérito.

Portanto, como o inquérito promovido pela Corte tem como objeto a apuração de ataques sistemáticos contra Corte, por meio de notícias falsas – mais ainda após as diligências de busca e

apreensão em que se apurou a existência de uma organização criminosa com o fim de propagar discurso de ódio contra as instituições democráticas e autoridades públicas – tem-se que o procedimento administrativo não fere os princípios da livre manifestação do pensamento e de expressão.

6 CONCLUSÃO

Por todas as razões elencadas neste presente trabalho, defende-se a relevância da pluralidade de ideias – da livre manifestação do pensamento e de expressão, de informação, de reunião e de associação – sendo imprescindível para consolidação de um Estado Democrático de Direito.

Assevera-se que liberdade de expressão nada tem a ver com as ditas *fake news*, uma vez que estas têm como objetivo ludibriar, enganar, denegrir pessoas, grupos e instituições, movendo a opinião pública contra as instituições democráticas e suas balizas constitucionais, rompendo com os princípios e os direitos fundamentais previstos na Constituição, a fim de beneficiar pessoa e/ou grupo específico.

Por último, afirma-se que o inquérito 4781 encontra guarida constitucional e infraconstitucional, uma vez ser promovido para defesa do Poder Judiciário – principalmente do STF e de seus ministros –, além das demais instituições democráticas, a fim de salvaguardar o sistema democrático brasileiro.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://tinyurl.com/czskwlw. Acesso em 01/06/2020.

BRASIL. **Emenda Constitucional n. 26**. Convoca Assembleia Nacional Constituinte e dá outras providências. Disponível em: https://tinyurl.com/ybvhpzj7. Acesso em 01/06/2020.

BRASIL. **Código de Processo Penal**. Disponível em: https://tinyurl.com/y37ko4qy. Acesso em 01/06/2020.

BRASIL. **Supremo Tribunal Federal**. Disponível em: https://tinyurl.com/y9o69zzj. Acesso em 01/06/2020.

BRASIL. **Tribunal Superior Eleitoral**. Disponível em: http://www.tse.jus.br/. Acesso em: 01/06/2020.

BRASIL. **Regimento Interno do Supremo Tribunal Federal**. Disponível em: https://tinyurl.com/gnmv7qq . Acesso em 02/06/2020.

BRASIL. **Ministério Público Federal**. Disponível em: http://www.mpf.mp.br/

Acesso em: 02/06/2020.

BRASIL. **Lei n. 6.683/1979**. Disponível em: https://tinyurl.com/y9uqlgga. Acesso em 01/06/2020.

BURKHARDT, Joanna M, **History of Fake News**. Disponível em: https://tinyurl.com/yctqgv4a. Acesso em 05/06/2020.

Convenção Americana de Direitos Humanos. Disponível em: https://tinyurl.com/yclqj585. Acesso em 01/06/2020.

Declaração dos Direitos do Homem e do Cidadão de 1789. Disponível em: https://tinyurl.com/k96tkbt. Acesso em 01/06/2020.

Declaração Universal dos Direitos Humanos. Disponível em: https://tinyurl.com/ycnawact. Acesso em 01/06/2020.

LIMA, Larissa Pinho de Alencar. **Acesso à comunicação virtual é um direito fundamental**. Conjur. 09/07/2012. Disponível em: https://tinyurl.com/yaacxomz. Acesso em 02/06/2020.

ORWELL, George. **1984**. Publicado em 1949, Editora Companhia das Letras.

PIOVESAN, Flávia e outros, **Impacto das Decisões da Corte Interamericana de Direitos Humanos na Jurisprudência do STF**. Salvador: Ed. JusPodivm, 2020.

PACELLI, Eugênio. **Em defesa do STF e dos tribunais**. Jota. 28/05/2020. Disponível em: https://tinyurl.com/ybuzy2t5. Acesso em 02/06/2020.

STRECK, Lênio. **Inquérito judicial do STF: o MP como parte ou "juiz das garantias"?**. Conjur. 28/05/2020. Disponível em: https://tinyurl.com/y9vmupdu. Acesso em: 03/06/2020.

VIEIRA, Oscar Vilhena. **Supremocracia**. Revista DIREITO GV 8. Disponível em: https://tinyurl.com/y9f5fbct. Acesso em 01/06/2020.

A FACILITAÇÃO DO CRIME DE INCITAMENTO A DESOBEDIÊNCIA, A INDISCIPLINA OU A PRÁTICA DO CRIME MILITAR POR MEIO DA

Daniel Passarella Roppa Arantes[1]

RESUMO

O Direito Penal Militar é, sem dúvida, extremamente contagiante e aclamado por grandes profissionais do Direito Brasileiro, apesar de severamente esquecido quanto a formação do Bacharelado em Direito. A adequação da legislação castrense é uma das necessidades mais importantes para o cotidiano de que aplica-a e, conforme adentramos em um espaço temporal onde as circunstâncias criminológicas se aperfeiçoam, como da prática de crimes digitais, na medida que buscam a impunidade, então, assim como na legislação penal comum, o CPM carece de tamanha necessidade de transformação também.

Palavras-chave: Crime Militar. Código Penal Militar. Crimes Digitais. Justiça Militar.

ABSTRACT

Military Criminal Law is, without a doubt, extremely contagious and acclaimed by great professionals of Brazilian Law, despite being severely forgotten about the formation of the Bachelor of Laws. The adequacy of military legislation is one of the most important needs for the daily life of which it is applied and,

[1] Bacharel em Direito. Professor de Direito Penal e Processo Penal Militar da Editora Avançar Educação. Aluno da pós-graduação *lato sensu* do Centro Universitário de Brasília – UniCEUB/ICPD. Formado em Direito na Universidade Cândido Mendes-RJ.

as we enter a time space where criminological circumstances are improved, such as the practice of digital crimes, as they seek impunity, then, as in common criminal law, the CPM also lacks such a need for transformation.

Keywords: Military Crime. Military Penal Code. Digital Crimes. Military Justice.

1 INTRODUÇÃO

O ramo especializado do Direito Penal Militar é, além do mais antigo no mundo, é o mais antigo do Brasil, sendo a Justiça Militar da União a primeira a ser realmente criada com o Conselho Supremo Militar e de Justiça, em 1º de Abril de 1808, pelo então Príncipe Regente, à época, D. João VI.

Várias modificações ocorreram posteriormente até que, com a CRFB/88, e com a vigência do Estado Democrático de Direito, a Justiça Militar não é apenas uma, mas sim duas, sendo dividida em Justiça Militar dos Estados e Justiça Militar da União. Tanto em um, como em outro, a 1ª instância é responsável pelo conhecimento do processo, sendo que será julgado por um colegiado de juízes, sendo um deles Juiz de Direito do Juízo Militar, no caso dos Estados, ou Juiz Federal da Justiça Militar, no caso da União, enquanto os demais serão militares. A depender do grau hierárquico, os militares serão julgados no Conselho Especial de Justiça, para oficiais, ou no Conselho Permanente de Justiça, para as praças. Já na 2ª instancia, para os estados, conforme o art. 125 §3º[2] da Constituição Federal, nós estaremos diante do Tribunal de Justiça Estadual ou Tribunal de Justiça Militar – a existência deste depende de proposta do Tribunal de Justiça do respectivo estado e que tenha mais de 20 mil militares, corpo de bombeiros militares e

[2] BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em 23/05/2020

polícia militar, em situação de atividade – e, na Justiça Militar da União, competirá ao Superior Tribunal Militar julgar, quando não originariamente, os recurso provenientes dos Conselhos de Justiça.

Contudo, as legislações castrenses em sua ótica penal – Código Penal Militar e o Código Processual Penal Militar – caminham a passos lentos, seja porque não há interesse dos legisladores em adaptar a norma, seja porque há o desprezo pelo ramo, advindo desde a época do período do Governo Militar de 1964.

Neste aspecto, lanço a compreensão da disciplina, em sua análise estrutural, e a discussão quanto ao Crime Militar de Incitamento (art. 155 do CPM)[3] que, por meio da facilitação da internet, auxilia na instigação da desordem, da desobediência e da indisciplina.

2 CRIME MILITAR E SEU CONCEITO ANALÍTICO

Apesar da palavra "PENAL", o CPM em muito se diferencia do Direito Penal Comum que estamos acostumados a estudar e aplicar diariamente. De certo que, para entender o crime militar, é necessário, antes de mais nada, compreender que militar não é meramente uma pessoa que usa farda e que presta continência e outros sinais de honra em seu dia a dia. O conceito de militar é, antes de mais nada, uma mescla do direito administrativo com as diretrizes e valores perpetuados pela Instituição Militar. Dessa forma, de forma objetiva, militar, em cargo efetivo ou temporário, é aquele servidor público, seja estadual ou federal, que está em atuação pelo estado, muitas vezes todos os dias da sua vida,

[3] BRASIL. Código Penal Militar (Decreto-Lei n. 1.001/69). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm>. Acesso em 22/05/2020.

devendo se subordinar a hierarquia e a disciplina como norte irrefutável de sua conduta. Segundo Cícero Robson Coimbra Neves, são valores intrínsecos da organização militar como um todo[4], o que aborda um entendimento de que o militar, sempre está em observância a estes princípios, inclusive quando ingressa na reserva, exceto aqueles que não sejam remunerados. E, se engana aquele que pensa que isso é apenas direcionado com o fim de cumprimento regulamentar. Negativo! Para fins penais também será considerado, principalmente, as prerrogativas de superior, em que diversas vezes, compõe o núcleo essencial do tipo penal militar, devendo ser observado, como já dito, ao militar da reserva, conservando nele as prerrogativas quando se pratica, ou quando contra ele é praticado (art. 13 CPM)[5].

Por outro lado, no que tange ao civil, devemos observar a ele não cabe esses valores quando está em prática do crime militar. Isso, contudo, não impede de que cometa crime militar, apenas em âmbito da JMU, já que a própria constituição trouxe em seu art. 124, *caput*, a redação que alarga a aplicação quanto ao sujeito ativo do crime militar[6], devendo observar, no entanto as demais exigências que a lei penal militar, no caso o CPM, dispor.

Por fim, feita as devidas informações quanto aos sujeitos do crime militar, devemos agora passar para o próximo tópico que é a

---

[4] NEVES, Cícero R. C.; STREIFINGER, Marcelo. *Manual de Direito Penal Miliar*. São Paulo: Saraiva, 2014. p. 39

[5] BRASIL. Código Penal Militar (Decreto-Lei n. 1.001/69). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm>. Acesso em 23/05/2020.

[6] O civil, for força do art. 125 §4º da CRFB/88 é claro ao dizer que, na JME, "*Compete à Justiça Militar estadual processar e julgar os militares dos Estados, nos crimes militares definidos em lei (...)",* restringindo dessa forma o campo de sua atuação apenas à Polícia Militar e ao Corpo de Bombeiros Militares. Já na JMU, conforme art. 124 *cáput* da CRFB/88, "*Compete à Justiça Militar processar e julgar os crimes militares definidos em lei"*, o que prevalece o entendimento de que não se restringe o âmbito de sua atuação, colocando todos como sujeitos possíveis de cometer o crime militar

conceituação do crime militar como um *fato típico, antijurídico e culpável*, devendo se enquadrar na *tipicidade indireta*, que é o art. 9º, e a adoção da *Teoria Causalista Neoclássica.*[7]

2.1 Fato típico

Parafraseando Cleber Masson, o conceito de fato típico é o fato humano que se enquadra com a perfeição aos elementos descritos pelo tipo penal[8]. Por outro lado, devemos destacar que, apesar de brilhante definição, no CPM, há algumas diferenças que são importantes destacar para compreendermos os diversos dispositivos da legislação castrense.

Em relação ao dolo e a culpa, devemos mencionar a sua ausência destes na prática da conduta, mas presentes na culpabilidade, o que caracteriza totalmente a teoria causalista, mas de forma *neoclássica*. Sem entrar muito na questão da culpabilidade, pois abordaremos mais à frente, a diferença para a teoria que adotamos em relação a teoria clássica, é que nesta não há elementos normativos, sendo puramente psicológica, ao contrário da legislação castrense em que temos a presença da imputabilidade (art. 48) e a exigibilidade de conduta diversa (art. 38) como um dos requisitos legais da culpabilidade, juntamente com a parte psicológica que é o dolo e a culpa.[9]

Nos demais requisitos do fato típico, no que tange ao resultado naturalístico, a relação de causalidade e a tipicidade, tirando algumas especialidades no que se refere ao crime tentado, tudo se assemelha com relação ao Código Penal Comum.

---

[7] NEVES, Cícero R. C.; STREIFINGER, Marcelo. *Manual de Direito Penal Miliar*. São Paulo: Saraiva, 2014. p. 201

[8] MASSON, Cleber. *Código Penal Comentado.* Rio de Janeiro: Forense; São Paulo: MÉTODO, 2018. p. 82

[9] NEVES, Cícero R. C.; STREIFINGER, Marcelo. *Manual de Direito Penal Miliar*. São Paulo: Saraiva, 2014. p. 461

2.2 Antijuricidade

Como todo elemento presente na conceituação analítica de crime militar, a antijuricidade não iria, ficar de lado no que se refere as características especiais advindas da natureza militar. A ilicitude ou antijuricidade é o elo de contrariedade entre o fato típico e o nosso ordenamento jurídico. É um juízo posterior ao da tipicidade e, para que deixe de ser crime, há de existir alguma das excludentes previstas no CPM.

As excludentes que o CPM traz em seu bojo são taxativas e, além das que já conhecemos por meio do Código Penal Comum como Estado de Necessidade, Estrito Cumprimento do Dever Legal, Exercício Regular do Direito e a Legítima Defesa, temos também a Excludente do Comandante e o Estado de Necessidade Exculpante, sendo que esta exclui a culpabilidade.

2.3 Culpabilidade

A culpabilidade, como mencionamos anteriormente, é definida conforme a *Teoria Causalista Neoclássica*, como *psicológica normativa*, visto que aloca-se nela o dolo e a culpa, a imputabilidade e a exigibilidade de conduta diversa.

A culpabilidade, conforme o Código Penal comum, é vazia e aborda a *teoria finalística* em que, o dolo e a culpa são alocados na conduta, no fato típico, contendo apenas elementos normativos. A grande comprovação deste entendimento, conforme Cléber Masson, foi adotada após a Reforma da Parte Geral pela Lei 7.209/1984, previsto especificamente no art. 20, *caput:*

> O CP em vigor, com a Reforma da Parte Geral pela Lei 7.209/1984, parece ter manifestado preferência pelo finalismo penal. Uma forte evidência se encontra no art. 20, caput – o erro sobre o elemento constitutivo do tipo legal de

> crime exclui o dolo, mas permite a punição pelo crime culposo, se previsto em lei. Ora, se a ausência de dolo acarreta na exclusão do fato típico (ainda que somente na forma dolosa), é porque o dolo está na conduta do agente, que deixa de ser dolosa para ser culposa"[10]

E, para confirmar que o CPM adotou a causalista neoclássica, também é possível corroborar este entendimento com a extração do art. 33 do CPM que dispõe sobre os elementos de dolo e culpa na culpabilidade:

> Art. 33. Diz-se o crime:
>
> I - doloso, quando o agente quis o resultado ou assumiu o risco de produzi-lo;
>
> II - culposo, quando o agente, deixando de empregar a cautela, atenção, ou diligência ordinária, ou especial, a que estava obrigado em face das circunstâncias, não prevê o resultado que podia prever ou, prevendo-o, supõe levianamente que não se realizaria ou que poderia evitá-lo.

Além disso, corroborando na doutrina, nas palavras de Cícero Robson Coimbra Neves:

> "Por outro lado, o Código Penal Castrense, fruto de primoroso Anteprojeto do Prof. Ivo D'Aquino e de cuidadoso trabalho da Comissão Revisora (composta, além do autor do Anteprojeto, pelos Profs. Benjamin Moraes Filho e José Telles Barbosa), foi inovador em vários institutos, entre os quais podem ser citados a teoria diferenciadora do estado de necessidade e a inauguração do sistema vicariante em matéria de medidas de segurança, em substituição ao sistema duplo binário, no que a legislação penal comum somente se igualou por ocasião da reforma da Parte Geral do Código Penal, em 1984, reforma essa trazida pela Lei n. 7.209, de 11 de julho daquele ano, e que não alcançou o Código Penal Militar de 1969, de sorte que podemos falar, com a vênia dos rigorosos estudiosos do Direito Penal, em "Direitos Penais

[10] MASSON, Cleber. *Código Penal Comentado.* Rio de Janeiro: Forense; São Paulo: MÉTODO, 2018. p. 83

> brasileiros", já que o Direito Penal comum, assim é enxergado majoritariamente, é informado pelo sistema finalista, impulsionado com a reforma em comento, enquanto o Código Penal Militar, que não foi afetado pelas inovações da década de 80, repousa sobre uma base **causalista neoclássica**"[11]

2.4 Tipicidade indireta (art. 9º, I, II, III)

A tipicidade indireta é o elemento mais importante do conceito analítico do crime militar, previsto no art. 9º do CPM, que é dividido em três incisos, sendo que no II e no III, deve-se ainda se atentar às respectivas alíneas. Pela natureza do delito e pelas circunstâncias, no sentido de tempo, pessoa e lugar, se estiverem presentes tais requisitos, então, de fato, aquele crime cabe à Justiça Militar processar e julgar. Neste sentido, Antônio Fernandes cita:

> "**Examinando-se os três incisos do art. 9o, percebe-se que os crimes militares são de tipificação direta e tipificação indireta**. Segundo o inc. I, para os crimes militares próprios basta a descrição típica da Parte Especial: tem-se aí crimes de tipificação direta. Mas os crimes impropriamente militares exigem, para sua tipificação, além dos elementos descritos na Parte Especial, outros dados que constam das alíneas do inc. II. Também são de tipificação indireta os crimes do inc. III, caracterizados pela conjugação dos elementos da descrição típica da Parte Especial com os elementos que o inciso contempla"[12]

Contudo, para entender melhor cada inciso, é necessário compreender os critérios específicos do crime militar[13], que se dividem em: ratione materiae, ratione personae, ratione locci, ratione temporis e ratione legis.

[11] NEVES, Cícero R. C.; STREIFINGER, Marcelo. *Manual de Direito Penal Miliar*. São Paulo: Saraiva, 2014. p. 43
[12] FERNANDES, Antônio Scarance. *Processo penal constitucional*. São Paulo: Revista dos Tribunais, 2007. p. 161
[13] Nomenclatura de minha autoria

O primeiro critério se dá em razão da natureza do crime[14], que é a parte essencial do crime militar, como por exemplo aqueles que se destacam pelas situações de ação militar, função militar, etc. Já o segundo critério, narra a possibilidade de reconhecer o crime militar pela pessoa contra quem está cometendo crime em específico, sendo, porém, a menos preponderante entre os demais critérios. Já o terceiro, traz a ideia do local onde tenha acontecido o crime militar, ou seja, local sujeito a administração militar. O quarto critério é em relação ao momento que prepondera para que ocorra o crime militar, como no caso de período de manobras. E, por último, o critério ratione legis, o qual seria o resumo de todos estes critérios, definindo como crime militar aquele tipo penal previsto em lei.

Tendo sido explicado cada um dos critérios, devemos então entrar no conteúdo mais importante da disciplina, que é o conceito legal de crime militar em tempo de paz, que é nosso enfoque, previsto no art. 9º e demais incisos,

2.4.1 Art. 9º, inciso I – militari tantum[15]

O inciso I é a definição legal de crime militar pela natureza do delito. Facilmente perceptível no momento que o dispositivo define como aqueles que estejam previstos apenas no CPM:

> Art. 9º Consideram-se crimes militares, em tempo de paz:
>
> I - os crimes de que trata este Código, quando definidos de modo diverso na lei penal comum, ou nela não previstos, qualquer que seja o agente, salvo disposição especial.

[14] NEVES, Cícero R. C.; STREIFINGER, Marcelo. *Manual de Direito Penal Miliar*. São Paulo: Saraiva, 2014 p. 89

[15] Nomenclatura de minha autoria, considerando serem esses puramente militares. Não confundir com propriamente militares, apensar da semelhança etimológica.

Trata-se do critério ratione materiae, no qual a sua aplicação advém na natureza militar em si. São crimes desta maneira o motim (art. 149 do CPM), deserção (art. 187 do CPM), insubmissão (art. 183 do CPM), dentre outros, e que estão previstos apenas no CPM ou de modo diverso do que prevê a legislação penal comum. Além disso, se analisarmos a disposição prevista no inciso I do art. 9, veremos que independe do agente que cometa o crime, podendo ser civil ou militar. Claro que, de certa forma, é necessário entendermos duas circunstâncias nesse aspecto. Uma que, como já falamos, no caso de um crime que, pela sua redação prevista no tipo penal, seja possível a pratica da conduta por um civil, apenas será possível exigir da Justiça Militar a competência quando for em detrimento de bens ou a ordem administrativa militar, ou os demais militares que compõem as Forças Armadas, ambos parte da Instituição Militar Federal como um todo. Ou seja, como dissemos anteriormente, o processamento e julgamento de crime militar cometido por civil apenas será possível em âmbito da JMU. Outro ponto, é que para passar pelo inciso que estamos comentando, no caso de civil, ele deve, obrigatoriamente, passar primeiro pelo inciso III, pois, como veremos mais à frente, obriga-o a se enquadrar em uma das circunstâncias nas alíneas previstas nele.

Por fim, não deixar de mencionar que o inciso I não necessita de qualquer complementação, como ocorre com os incisos II e III, que dependem de outros critérios específicos em cada uma de suas alíneas

2.4.2 Art. 9º, II – crimes militares por extensão

É o dispositivo que mais sofreu alteração e, com total certeza, é a principal mudança no CPM, dede 1969, ano de sua criação.

O dispositivo foi alterado pela Lei 13.491/2017, na qual passou a considerar não só os crimes que tenham mesma redação no CPM e os previstos na legislação penal comum, mas também aqueles que estejam previstos apenas nestas. Isso fez com a doutrina classifica-se estes últimos como *crimes militares por extensão*[16], conforme posição de Jorge César Assis. Sendo assim, qualquer crime que esteja previsto em outra legislação penal, e que satisfaça os requisitos presentes em uma das alíneas do inciso II, será crime militar também. Com bastante entusiasmo, digo que isso possibilitou uma ampliação da Justiça Militar, deixando a cargo dela, como sempre deveria ser, a competência de julgar aqueles servidores regrados pelo militarismo e seus valores. Outro dispositivo modificado, mas que falaremos mais à frente, são os crimes dolosos contra a vida de civil, no exercício da função militar e por militares das forças armadas, que passaram a ser de competência da Justiça Militar da União. Todas essas modificações, de cunho material e processual, diante da alteração da competência, deram a legislação uma natureza híbrida, conforme posicionamento corroborado pelo STJ:

> CONFLITO NEGATIVO DE JURISDIÇÃO. JUSTIÇA FEDERAL E JUSTIÇA MILITAR. CRIME CONTRA A LEI DE LICITAÇÕES PRATICADO CONTRA PATRIMÔNIO SOB A ADMINISTRAÇÃO MILITAR. SUPERVENIÊNCIA DA LEI N. 13.491/17.

[16] ASSIS, Jorge Cesar de. Crime militar & processo: comentários à Lei 13.491/2017. Curitiba: Juruá, 2018. 48

> A Lei n. 13.491/17 promoveu alteração na própria definição de crime militar, o que permite identificar a natureza material do regramento, mas também ampliou, por via reflexa, de modo substancial, a competência da Justiça Militar, o que constitui matéria de natureza processual. Como a lei pode ter **caráter híbrido** em temas relativos ao aspecto penal, a aplicação para fatos praticados antes de sua vigência somente será cabível em benefício do réu, conforme o disposto no art. 2º, § 1º, do CPM e no art. 5º, XL, da CF/88. Por sua vez, no que concerne às questões de índole puramente processual - hipótese dos autos -, o novo regramento terá aplicação imediata, em observância ao princípio do tempus *regit actum*. Precedente.[17]

Pois bem, dando continuidade, para que seja considerado crime militar, devemos fazer a observação frente as alíneas "a", "b", "c", "d" e "e". Cada uma delas obedece um requisito que devemos nos atentar para poder classificar como crime militar

A alínea "a", diz que será crime militar em tempo de paz, quando praticado por militar em situação de atividade contra militar na mesma situação. Importante lembrar que *situação de atividade* não é exercício da função, mas sim em relação ao militar que tenha se aposentado, compulsoriamente ou a pedido, ou melhor, cumprido o tempo de serviço exigido em lei. O termo aposentado no militarismo é usado de maneira diferente, no qual chama-se de *inatividade*, composta por militares da *reserva*, que a qualquer momento, em tempo de crise, pode vir a ser chamado para compor um efetivo em guerra, e os da *reforma*, que são aqueles que estão dispensados de qualquer efetivo, em caso de guerra. Porém, apesar de saber disso, várias jurisprudências têm demonstrado total desencontro com esta verdade, o que tem acarretado desconhecimento e insipiência por parte de quem está operado o direito penal militar. Por sorte o entendimento que

[17] STJ, CC 160.902/RJ, Terceira Seção, Rel. Min. Laurita Vaz, DJe 18/12/2018.

predomina é do STM, no qual corrobora exatamente que militar, em situação de atividade, contra outro militar na mesma situação, será crime militar, independente de folga ou qualquer outra predominância, bastando o critério *ratione personae*:

> EMENTA: APELAÇÃO. DPU. ART. 240 DO CPM. FURTO DE VEÍCULO AUTOMOTOR. PRELIMINAR. INCOMPETÊNCIA DA JMU PARA JULGAR O FEITO. REJEITADA. MÉRITO. FINALIDADE DO AGENTE DELITIVO. DETENÇÃO DA RES FURTIVA. ESFERA DE VIGILÂNCIA DA VÍTIMA. SUBTRAÇÃO CONSUMADA. FURTO DE USO. TENTATIVA. DESCARACTERIZAÇÃO. APELO NÃO PROVIDO. UNANIMIDADE. 1. Preliminar. Considera-se *militar* em situação de atividade aquele que está no serviço ativo "da *ativa*", "em atividade", não importando se está de *folga*, à paisana, de férias ou em local que não seja sujeito à Administração Militar. Ademais, o local de consumação do delito e a existência de liame com a função *militar* são irrelevantes para a configuração do crime castrense, bastando que esteja presente o critério ratione personae.[18]

Já na alínea "b", no qual será crime militar em tempo de paz a conduta praticada por militar da ativa, ou em situação de atividade, em local sujeito a administração militar, contra militar da reserva, reformado ou civil. Na presente classificação, nós temos o critério *ratione locci*, ou seja, o crime militar apenas se completa, nos ditames do art. 9º, II, se cometido em local sujeito a administração militar. E o que vem a ser local sujeito a Administração Militar? Existem várias definições do que seria este lugar, uns definindo como o quartel, outros definindo como uma sede administrativa. Porém, dentre diversas, a que mais se identifica, para apresentar de forma objetiva este artigo, é a definição de Jorge Alberto Romeiro. Segundo o autor, o conceito se define como espaço físico em que as forças militares realizam suas

[18] STM, AP 7000026-56.2018.7.00.0000, Rel. Min. Carlos Augusto de Sousa. 17.12.2018

atividades, como quartéis, aeronaves, embarcações, estabelecimentos de ensino militar, campos de treinamento, etc.[19]

Na alínea "c", nós temos o critério *ratione materiae*, no qual será considerado crime militar em tempo de paz, o militar da ativa que comete crime militar contra militar inativo ou civil, independentemente de estar em local sujeito à administração militar, mas que aquele esteja *em serviço*, *atuando em razão da função* ou *em comissão de natureza militar*, ou *em formatura*. Agora, sim, senhores, podemos enxergar a presença da atividade militar, ou seja o exercício da atividade militar.

Em continuidade, na alínea "d", nós temos o crime militar em razão do momento, ou seja, quando ocorre. No caso, estamos tratando do critério *ratione temporis*, sendo que, conforme o dispositivo legal, será crime militar em tempo de paz aquele fato praticado por militar da ativa contra militar inativo ou civil, durante o período de manobras ou exercício. Segundo a excepcional doutrina de Cícero Robson Coimbra Neves, o período de manobras ou exercício deve ser entendido como o espaço temporal compreendido entre o aprontamento da tropa até sua liberação[20].

Por fim, a alínea "e" é aquela destinada aos crimes militares praticados por militar da ativa contra o patrimônio sobre a administração militar, ou contra a ordem administrativa militar. Pela natureza do patrimônio e pelo tipo de ordem que é posta em prejuízo, é possível ver que o critério utilizado para classificação do crime militar é o *ratione materiae.*

[19] ROMEIRO, Jorge Alberto. Curso de Direito Penal Militar: *Parte Geral*. São Paulo: Saraiva, 1994. p. 79

[20] NEVES, Cícero R. C.; STREIFINGER, Marcelo. *Manual de Direito Penal Miliar*. São Paulo: Saraiva, 2014

2.4.3 Art. 9º, III – eximia agentibus[21]

Supracitando aquilo que já foi dito várias vezes, o civil não está isento de responder na Justiça Militar, porém, apenas no que tange a detrimento da Instituição Militar em âmbito Federal. O inciso III trará como agentes ativos do crime militar, os militares inativos, da reserva e da reforma, e o civil, sendo que, como regra geral, devem, acima de tudo, ferir de forma objetiva a Instituição Militar, além de se enquadrarem em uma das alíneas daquele. Este é o entendimento que predomina no STM:

> EMENTA: RECURSO EM SENTIDO ESTRITO. MPM. ROUBO DE VEÍCULO DO EXÉRCITO BRASILEIRO. COMPETÊNCIA DA JUSTIÇA MILITAR DA UNIÃO PARA JULGAR CIVIS. 1. À JMU não cabe julgar somente os integrantes das Forças Armadas, mas todos os agentes que tenham praticado crimes definidos na legislação penal militar, incluindo os civis. 2. A fixação da competência da Justiça Militar da União não decorre da ciência do agente acerca da propriedade da res furtiva ou da demonstração de sua intenção em ofender as *instituições militares*, bastando, para tanto, o atentado ao patrimônio sob a administração militar, pois o art. 9º, III, alínea "a", do CPM, apresenta ***critérios objetivos*** e não faz tal ressalva. Preliminar rejeitada. Decisão unânime. Recurso conhecido e provido. Decisão unânime[22].

Na primeira alínea, nós temos o que seria algo parecido com que vimos na alínea "e" do inciso II, mas agora com outros agentes no poli ativo. Serão crimes militares em tempo de paz aqueles cometidos por militar inativo ou civil, contra o patrimônio sob a administração militar ou contra a ordem administrativa

[21] Nomenclatura de minha autoria, visto que se adequa a uma classificação por agentes que cometem crime militar mas excepcionalmente, visto que não são militares em situação de atividade ou, muito menos, militares em si.

[22] STM, RSE 7000452-34.2019.7.00.0000, Rel. Min. Arthur Vidigal de Oliveira. 21.08.2019

militar. Segue-se o critério em razão da matéria e especialidade militar

Na alínea "b", temos como crime militar em tempo de paz quando praticado por militar inativo ou civil, em local sujeito a administração militar, contra militar da ativa, ou contra funcionário de Ministério Militar ou da Justiça Militar, no exercício da função inerente ao cargo. A observação que deve-se fazer é que não existe mais Ministério Militar, sendo que hoje temos o Ministério da Defesa, e que a disposição no que tange aos funcionários da Justiça Militar, tem que ser analisada, no âmbito da ótica constitucional, como não recepcionado, visto que a JMU é órgão do Poder Judiciário e não se deve fazer um paralelo com os militares, visto que ambos seguem regulamentos distintos e são subordinados a diferentes poderes. A alínea supracitada obedece a classificação do *ratione locci*, não sendo um equívoco as pessoas comumente classificar como *ratione locci* e *ratione personae*, diante do fato de ser praticado contra militar da ativa.

Seguindo, na alínea "c", nós temos o crime militar em tempo de paz quando militar inativo ou civil pratica-o contra militar da ativa que esteja em formatura ou em período de prontidão, vigilância, observação, exploração, exercício, acampamento ou manobras. Apesar de muitos termos específicos, basta entender que remete-se ao fato de ser *ratione materiae* e/ou *ratione temporis*, visto que trata-se de uma atividade típica de militar ou que acontece em determinado período.

Por fim, ocorrerá crime militar em tempo de paz, conforme a alínea "d", quando militar inativo ou civil pratica-o, ainda que fora de local sujeito à administração militar, contra militar em função de natureza militar, ou que esteja no desempenho de serviço de vigilância, garantia e preservação da ordem pública, administrativa

ou judiciária, quando for legalmente requisitado para esta atividade, ou em obediência à determinação legal superior. Ou seja, aquele irá cometer o crime, independente do lugar que esteja, mas desde que, ao atingir o militar esteja em serviço de função militar ou em atividade que se relacione com a atividade de Garantia da Lei e da Ordem – GLO – determinada por autoridade superior, no caso, o Presidente da República. Esta hipótese relaciona-se com o critério *ratione materiae* e/ou *ratione personae*.

3 INCITAMENTO AO CRIME MILITAR DIGITAL

Feita uma breve análise do que seria os crimes militares e seu conceito analítico, passemos agora para uma análise mais aprofunda pelos crimes militares em espécie e a problemática por trás das facilidades em usar os meios digitais para praticá-los em prejuízo da disciplina e hierarquia militar.

3.1 Dos crimes militares contra a disciplina e autoridade em meio às redes sociais

Os crimes previstos no Título II do CPM, tratam dos crimes em que a os bens jurídicos tutelados, seja de forma alternativa ou cumulativa, são a disciplina e a autoridade militar, nos quais, de forma unânime, o sujeito passivo sempre será o Estado. O principal crime caracterizado neste Título é, sem dúvida, o crime de *motim* (art. 149 do CPM) – *reunirem-se dois ou mais militares para agindo em desobediência ou desordem* -, no qual é crime de *concurso necessário*, nos quais exige-se, para sua configuração, mais de um agente no polo ativo. É *crime propriamente militar*[23], pois apenas militares da ativa podem cometer o crime militar, já

[23] Crime propriamente militar é aquele que, de acordo com a Teoria Clássica, apenas o militar poderá cometer o crime. A tipicidade indireta pressupõe o art. 9º, I do CPM

que assim exige a redação do tipo penal, mas que nada impede que o civil ou militar inativo participe ou seja coator, havendo no mínimo dois militares da ativa, conforme a comunicação das circunstâncias elementares do tipo penal militar prevista no art. 53 §1º do CPM. Neste caso, devemos entender que o artigo traz quatro incisos que caracterizam as condutas do tipo, sendo fato que, em todas formas, o militar age em desobediência ou em forma desordeira. O que gostaria de destacar é o previsto no inciso III, tratando-se da conduta de ***assentir*** em recusa conjunta de obediência, ou em *resistência* ou *violência*, em comum, contra superior. Repare que, por meio do verbo "assentir", podemos concluir que os agentes concordam ou ratificam a conduta de um militar que já age em recusa à obediência e, acreditando eles que devem fazer o mesmo, acabam instigando-se a participar da recusa em conjunto.

Veja que isso é totalmente possível por meio da internet, nas redes sociais, quando vemos um militar que, por meio de publicação nos *stories*[24], resolve exteriorizar ao mundo que se recusa a obedecer à escala de cumprimento de vigilância, em um determinado período. Ao ver isso, havendo outro(s) seguidor(es) do mesmo quartel e um ou mais de um acabam por assentir em concordância com aquele, se recusando a prestar também o serviço pelo qual foram escalados no mesmo dia, estaremos diante, dessa forma, de um crime militar de motim.

Outro crime que gostaria de analisar, e que se parece muito com o que comentamos acima, é o crime de *Incitamento* (art. 155 do CPM) – *incitar à desobediência, à indisciplina ou a prática de*

[24] Meio pelo qual o usuário publica um momento ou uma outra publicação de terceiro, sendo que a história permanecerá ativa por 24h, podendo ser tanto publicada a todos como apenas a alguns seguidores.

crime militar. É *crime impropriamente militar*[25], conforme a classificação da *Teoria Clássica*, ou seja qualquer um pode cometer o crime, visto que o dispositivo não trouxe nenhuma circunstância elementar que caracteriza-se um agente em específico. Outro ponto é que, conforme o §Ú, caso ocorra por meio introdução, afixamento ou distribuição, em local sujeito à administração militar, de impressos, manuscritos ou outros materiais de fotocópia ou mimeografado, também incorrerá na mesma pena do *cáput*, que reclusão de dois a quatro anos. Por outro lado, e no que se refere aos materiais que são publicados nas redes sociais? No meu entendimento, é perfeitamente possível a aplicação, da conduta com a forma prevista no art. 155, visto que, conforme a modernidade, a *internet* é, sem dúvida, o meio mais fácil de se propagar uma ideia e atingir uma demanda acima do que se espera. Neste contexto, podemos ver um militar das forças armadas que, em casa, de folga, e resolve, por meio do *Facebook*, por exemplo, incitar civis a praticarem crime de *ingresso clandestino* (art. 302 do CPM) no 1º RCG – *Regimento de Cavalaria de Guarda* – de administração do Exército Brasileiro, onde não há passagem regular. Ainda que os civis ou outros militares não queiram praticar o crime, já estará consumado a conduta, independente da invasão.

3.2 Majoração da pena como desencorajamento para à indisciplina e desobediência

Apesar de ir em caminho oposto ao que prega parte da doutrina no Direito Penal Comum, é de se vislumbrar que, por

[25] Crime impropriamente militar é aquele que, de acordo com a Teoria clássica, qualquer um poderá cometer o crime, apesar do crime estar previsto apenas no Código Penal Militar. Se cometido por militar da ativa, pressupõe a tipicidade indireta pelo art. 9º, I, porém, caso seja militar inativo ou civil, pressupõe-se que passe pelo art. 9º, III, ambos do CPM

estarmos em um ramo especializado do Direito, o agravamento em diversas circunstâncias no CPM é totalmente necessário para estabilizar a ordem e desestimular o agente para se manter dentro dos limites legais, sem olvidarmos, contudo, das garantias fundamentais inerentes ao indivíduo. O fato de haver um meio de encorajamento e incentivo à prática do crime militar, incluindo a indisciplina e a desobediência, é totalmente discutível nos dias de hoje, devendo por parte daqueles que estudam o Direito Penal Militar apresentar medidas de adequadas para evitar eventuais danos a Instituição Militar e a sociedade em si.

A forma de majoração da pena e reformulação do CPM é a medida mais adequada para trabalharmos na linha de estabilização da atividade delitiva. Alguns entendem que, após a Lei 13.491/2017, que trouxe os *crimes militares por extensão*, com a aplicação de crimes previstos nas legislações penais comum, respeitando as alíneas dos incisos II e III do art. 9º, não seria mais necessária uma adequação exclusiva no Direito Penal Militar, visto que a legislação castrense acompanhará a comum. Apesar da boa observação, quando tratamos de crimes previstos apenas na legislação penal comum, ou com igual definição no CPM, estamos tratando apenas dos *crimes impropriamente militares*, sendo que, conforme toda a extensão dos crimes militares em espécie, a sua maioria se trata de *crimes propriamente militares*. Estes, por sinal, estão apenas presente no CPM, e merecem também o respeito a uma adequação ao momento atual e a política criminal.

Além disso, devemos ter em mente que, como já supracitado, a disciplina e hierarquia são valores que se acrescentam a inúmeros dispositivos legais, seja em âmbito federal ou estadual, quando tratamos de militares. Dessa forma, a internet, por si só, é praticamente um submundo, ouso a dizer que

seria uma outra dimensão, na qual ainda não temos uma fiscalização - *NÃO CONFUNDAM COM REGULAMENTAÇÃO!* – para podermos ter mais tranquilidade com relação aos sítios eletrônicos que acessamos ou que estamos divulgando uma imagem nossa. Nesse sentido, também devemos lembrar que, em se tratando de redes sociais, também não há uma fiscalização totalmente eficaz que visa a identificação dos criminosos virtuais, principalmente no que tange aos crimes contra a honra. O detalhe é que, como estamos falando de crime militar, é possível verificar as inúmeras possibilidades de incitamento ao crime militar (art. 155 do CPM), ou mesmo a Prática de Ofensa às Forças Armadas (art. 219 do CPM) ou ainda ato oficial de superior ou do Presidente da República, por exemplo (art. 166 do CPM)[26]. Dessa forma, como não está de serviço ou, muitas vezes, não vendo seu superior, ou ainda, encorajado por conta da possibilidade do anonimato, o militar acaba praticando a conduta ilícita, além de poder incitar que outros façam o mesmo, já acreditam fielmente que estão exercendo uma manifestação do pensamento ou se aproveitando de uma circunstância em que não podem ser vigiados ou muitos punidos por isso.

Além dos termos citados, a crença na impunidade e na igual condição com o civil, o faz pensar e proliferar qualquer tipo de pensamento que desencadeie a desobediência e a indisciplina. A manifestação do pensamento, dentro do sentimento militar, deve ser mitigada com disciplina e hierarquia, somada ao princípio da baioneta inteligente. Isso significa que o militar, zelará pelos valores basilares dentro da Instituição Militar, mas que não se

[26] Lembrando que, para este crime apenas militar da ativa pode cometê-lo. Militar inativo ou civil não cometem o crime, podendo, entretanto, ser partícipes ou coautores, diante da comunicação de circunstâncias elementares do tipo penal militar.

submeterá ao ato manifestamente criminoso ou ilegal, diante do *princípio da baioneta inteligente*. Ao contrário, o civil apenas se atentará aos termos ilegais previstos na legislação penal e a mitigação com o direito fundamental de *liberdade de expressão*. Ou seja, totalmente desvinculado com outro valor de dependência disciplinar ou hierárquica.

Dessa forma, a fim de querer um melhor enquadramento das circunstâncias que norteiam os crimes militares, uma agravante genérica ou especial, a depender do crime, que se caracterize pelo cometimento do delito por meio da *internet*, seria totalmente útil e necessário. Além disso, se presumisse uma hipótese de aplicação de dispositivos gerais – *não a extensão dos crimes, pois esta é legal, diante da Lei 13.491/*2017 – presentes no Código Penal Comum, e que agravam a situação do criminoso, então estaríamos em contrariedade com a doutrina e a jurisprudência contemporânea que vedam no Direito Penal substantivo a aplicação da *analogia in malam partem*[27].

4 CONCLUSÃO

Apesar de toda o desmerecimento que, ao longo dos anos, a legislação penal militar tem sofrido, é certo que os mais novos doutrinadores, e me coloco nesse grupo renomado, estão procurando maneiras de trazer um encaixe perfeito ao nosso ordenamento jurídico, em conformidade com as diretrizes traçadas pela CRFB/88.

Os princípios sempre mencionados, hierarquia e disciplina, nunca serão administrados de forma isolada, sendo necessária a

[27] Aplicar um caso análogo em outra legislação ou na mesma, a fim de suprir uma lacuna. No Direito Penal, seja o comum ou o militar, é apenas aceito a analogia in bonam partem

apreciação conjunta e que delimita a atuação, em todo o momento, inclusive de folga e, em alguns casos, na inatividade do militar, independente onde esteja.

Por fim, a regulamentação, como estamos acostumados a ouvir, deve ser sempre divergida da fiscalização. Aquela sempre irá depender da ação estatal para colocar a mão em liberdades inerentes ao indivíduo e a coletividade. A segunda, trata de uma limitação no que tange ao acesso amplo à liberdade, mas sem que isso possibilidade abusar dos meios constitucionais, trazendo um entendimento de mitigação de relativismo dos Direitos Fundamentais. Essa, com certeza, é a forma mais justa de adequação ao nosso cotidiano frente as profundas mudanças que estamos passando, seja de forma intencional ou apenas por força da natureza.

REFERÊNCIAS

ASSIS, Jorge Cesar de. Crime militar & processo: comentários à Lei 13.491/2017. Curitiba: Juruá, 2018.

BRASIL. Código Penal Brasileiro (Decreto-Lei n. 2.848/40). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm>. Acesso em 29/05/2020

BRASIL. Código Penal Militar (Decreto-Lei n. 1.001/69). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm>. Acesso em 23/05/2020.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em 24/05/2020.

MASSON, Cleber. Código Penal Comentado. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2018

NEVES, Cícero R. C.; STREIFINGER, Marcelo. Manual de Direito Penal Miliar. São Paulo: Saraiva, 2014.

ROMEIRO, Jorge Alberto. *Curso de direito penal militar*: Parte Geral. São Paulo: Saraiva, 1994.

PICKPOCKET DIGITAL: A FACILIDADE DO PAGAMENTO POR APROXIMAÇÃO

Lana Aimée Brito de Carvalho[1]

RESUMO

O presente artigo científico tem como objetivo principal a análise e estudo da tecnologia NFC, que possibilita o pagamento por aproximação, e as consequências jurídicas decorrentes da má utilização nas operações financeiras. Pretende-se analisar, discutir e apresentar os principais aspectos que a sociedade enfrenta em relação à essa novidade do mundo digital e suas consequências jurídicas. Para isso, empregou-se a metodologia de pesquisa bibliográfica, utilizando-se como base a literatura doutrinária, jurisprudências, análises de artigos científicos e legislação específica referente ao tema exposto. Portanto, ao longo dos capítulos deste trabalho, será analisada a tecnologia NFC, sua regulamentação e os delitos empregados nessa forma de pagamento, visando concluir se é um meio de pagamento seguro.

Palavras-chave: NFC. Near field communication. Transação bancária.

ABSTRACT

The main objective of the following case-study is to analyze and study the NFC technology, which enables payment by approximation, and the legal consequences of misuse in financial

[1] Bacharel em Direito e aluna do curso de pós graduação *lato sensu* em Direito pelo Instituto Ceub de Pesquisa e Desenvolvimento – ICPD – do Centro Universitário de Brasília – UniCEUB.. E-mail: lanaaimee@gmail.com.

transactions. Using recent literature, this report seeks to analyze and present the main aspects that society faces in relation to this newness of the digital world and its legal consequences. This study was conducted using doctoral theses, jurisprudence, and legislation related to the exposed theme. Therefore, the next few chapters of this case study, NFC technology, it's regulation and the offenses employed in this form of payment will be analyzed, in order to conclude whether it is a secure means of payment.

Keywords: NFC. Near field communication. Bank transaction.

1 INTRODUÇÃO

O presente trabalho tem como proposta analisar o método de pagamento por aproximação sob o viés da criminalidade que esta inovação trouxe consigo, por conta de sua facilidade em finalizar as transações bancárias.

A tecnologia NFC, sigla para *Near Field Communication*, se tornou uma das mais promissoras tecnologias nos últimos anos, possibilitando o pagamento por aproximação, uma das principais tendências do mercado, uma vez que grande parte dos estabelecimentos de diferentes ramos empresariais disponibilizam essa opção e o dinheiro físico aos poucos está se tornando menos utilizado, de modo que o uso de outros meios de pagamento, como o cartão, tem sido cada vez mais frequente.

O NFC é uma tecnologia *contactless*, também conhecida como tecnologia por aproximação, que tem como principal função transmitir dados de forma rápida, apenas aproximando a uma distância de poucos centímetros ou encostando dois dispositivos eletrônicos compatíveis.

O método de pagamento digital é uma novidade para seus usuários que conseguem pagar uma conta sem precisar inserir ou passar o cartão na maquineta, bastando aproximar um dispositivo

a uma distância de meros centímetros para que a transação ocorra, muitas vezes não precisa nem digitar senha.

Essa facilidade em pagar por aproximação oferecida pelos bancos por meio dos dispositivos móveis e cartões, tem gerado preocupação para os especialistas em tecnologia e segurança e em seus clientes, posto que essa tecnologia está sendo aproveitada para a prática de pequenos delitos e começando a tomar proporções perigosas.

Nesse contexto, o objetivo do presente artigo consiste em compreender a dinâmica do NFC, seu uso e modalidades, além das consequências jurídicas decorrentes da má utilização dessa tecnologia nas operações financeiras.

O estudo se justifica pela atualidade do tema no contexto social, econômico e jurídico, uma vez que as relações que envolvem o processamento de pagamentos por produtos ou serviços e algumas transações financeiras hoje destacam o uso desse mecanismo, que possibilita a troca do dinheiro de uma forma diferente da tradicionalmente utilizada pelos bancos.

2 NFC (*NEAR FIELD COMMUNICATION*): ESCLARECIMENTOS NECESSÁRIOS

NFC é a sigla para *Near Field Communication*, que em português é traduzido como Comunicação por Proximidade de Campo. Esta tecnologia funciona com a radiofrequência, podendo ser usada à distância, normalmente de 0 a 10 cm entre os dispositivos.

Segundo a definição apresentada pelo NFC Fórum, trata-se de uma tecnologia que torna a vida mais fácil e conveniente, simplificando transações, trocas de conteúdo digital e conexões

entre dispositivos eletrônicos, com um toque ou a aproximação, eliminando a necessidade de procedimentos complexos e caros.[2] A ideia é que os usuários desta tecnologia sejam capazes de realizar uma comunicação rápida e segura entre vários dispositivos sem ter que dispender esforços em configurações de redes.

O NFC é uma rede de comunicação sem fio de curto alcance, desenvolvida pela Nokia Corporation, Sony Corporation e Royal Philips Electronics em 2002 e impulsionada a partir de 2004 depois da criação do Fórum NFC, que promoveu o avanço da tecnologia definindo especificações e regulamentações de uso.[3]

Desde então, com a adoção do NFC pela indústria, surgiram diferentes aplicações e serviços, tais como transações financeiras, emissões de bilhetes, transportes, serviços médicos, identificação, controle de acesso, distribuição de conteúdo, publicidade e transferência de dados.

A tecnologia pode ser utilizada para transmissão de pequena quantidade de dados, como informações de pagamento, cartões de visita, autenticação e iniciador de comunicação secundária, como *Bluetooth* ou *WiFi*.

Essa tecnologia é, ainda, compatível com dispositivos RFID (Identificação por Radiofrequência), que operam com a mesma frequência e modos de operação. Assim, os dispositivos habilitados com NFC são capazes de emparelhar cartões com a tecnologia RFID.

---

[2] NFC FORUM, 2013. Disponível em: <https://nfc-forum.org/>. Acesso em: 17 de maio de 2020.

[3] NASSAR, Victor; VIEIRA, Milton L.H.; *Método de Pesquisa para Análise da Experiência dos Usuários com a Tecnologia NFC (Near Field Communication)*. Universidade Federal de Santa Catarina, 2015. Disponível em: https://www.academia.edu/7160201/M%C3%A9todo_de_pesquisa_para_an%C3%A1lise_da_experi%C3%AAncia_dos_usu%C3%A1rios_com_a_tecnologia_NFC_Near_Field_Communication_. Acesso em: 16 maio 2020.

A comunicação entre os dispositivos é limitada a dois participantes, sendo um protocolo *peer-to-peer*, e apenas um dispositivo por vez pode transmitir seus dados, eis que os dispositivos compartilham uma única banda de radiofrequência. Assim, o dispositivo participante na comunicação deve primeiro constatar se não tem outro dispositivo transmitindo dados no momento para poder iniciar a sua comunicação.

2.1 Modos de operação

O NFC possui dois modos de operação, o ativo e o passivo. No modo de comunicação ativa, ambos os dispositivos são capazes de gerar e receber sinais de radiofrequência, já no modo de comunicação passivo, um dos dispositivos, o emissor, gera o sinal de radiofrequência e o outro dispositivo, o receptor, apenas recebe a informação.

A operação do NFC é feita por radiofrequência, trabalhando em 13,56 MHz e com distâncias de até 10 cm, sua frequência não é regularizada, não tendo restrições e nem sendo necessário licença para seu uso, assim, pode-se ter vários dispositivos na mesma área.[4]

Os dispositivos dotados de fonte de energia própria, como bateria ou energia elétrica convencional são os que possuem o modo de comunicação ativo, os leitores NFC são exemplos de dispositivos ativos.

No caso do modo de comunicação passivo, um campo eletromagnético é gerado e esse campo induz uma corrente elétrica no dispositivo passivo, que faz com que este tenha energia

[4] CRUZ, Kelly. *Estudo sobre o near field communication e seu papel em pagamentos via dispositivos móveis*. Trabalho apresentado no curso de pós-graduação em Rede de Computadores do Centro Universitário de Brasília - UniCEUB/ICPD, 2013.

para funcionar pelo tempo em que estiver sob a ação do referido campo, os cartões são exemplos de dispositivos passivos, pois conseguem apenas emitir informações e não receber.

Nesse contexto, a comunicação do NFC da transação bancária funciona no modo de operação ativo, na qual um dos dispositivos recebe a informação do emissor e, em seguida, emite a confirmação de pagamento para o mesmo equipamento.

2.2 O NFC no Brasil

O NFC se tornou uma das mais promissoras tecnologias nos últimos anos e é uma das principais tendências do mercado mundial, tendo em vista que possibilita o pagamento por aproximação, opção de pagamento que está sendo disponibilizada em grande parte dos estabelecimentos de diferentes ramos empresariais.

Os métodos de transferência bancária, TED (Transferência Eletrônica Disponível) e DOC (Documento de Ordem de Crédito), são atualmente vistos como ultrapassados e limitados, tendo em vista que os sistemas de transações bancárias que utilizam a tecnologia NFC são mais rápidos e econômicos, funcionando 24 horas por dia.

Nos Estados Unidos e no Japão, a tecnologia NFC já é utilizada para comprar bilhetes de trem e ingressos de eventos, fazendo parte do dia a dia de grande parte da população. Em Tóquio, é possível comprar passagens de metrô apenas aproximando um dispositivo móvel à catraca, já em Arizona,

alunos usam seus aparelhos celulares para ganhar acesso à prédios da Universidade.[5]

No Brasil, a tecnologia NFC foi introduzida pela PagSeguro em 2012, logo após, empresas de telefonia como a Claro, Vivo e Tim começaram a oferecer o serviço de pagamento móvel com o apoio dos bancos Bradesco e Itaú, bem como foi disponibilizado mais de 300 mil equipamentos com NFC pela empresa Cielo.[6] Assim, a partir de sua introdução no Brasil, grandes empresas se movimentaram e investiram na implementação da tecnologia NFC em seus produtos e serviços.

O NFC se mostra uma tecnologia vantajosa, tanto para consumidores como para comerciantes, por possibilitar conexões simples e rápidas de tecnologias sem fio, como o *Bluetooth* e o *Wi-Fi*, bem como pode ser usada em vários ramos industriais e ambientes.[7] À vista disso, estima-se que esta tecnologia domine o mercado, substituindo cartões e até dinheiro.

3 PAGAMENTO POR APROXIMAÇÃO

O pagamento por aproximação é realizado através de um dispositivo NFC, que pode ser um cartão *contactless* ou um aparelho móvel, possibilitando a seus usuários o acesso à vários serviços através de um único objeto.

[5] HECKE, Caroline. Onde e como a tecnologia NFC está sendo aplicada. *Tecnomundo*, 2011. Disponível em: <https://www.tecmundo.com.br/nfc/8173-onde-e-como-a-tecnologia-nfc-esta-sendo-aplicada.htm>. Acesso em: 18 de maio de 2020.

[6] VASQUES, Victor. PagSeguro lança serviço de NFC no Brasil, para pagamentos via celular. *Techtudo*, 2012. Disponível em: < https://www.techtudo.com.br/artigos/noticia/2012/04/pagseguro-lanca-servico-de-nfc-no-brasil-para-pagamentos-celular.html>. Acesso em: 16 de maio de 2020.

[7] NFC FORUM, 2013. Disponível em: <https://nfc-forum.org/>. Acesso em: 17/05/2020.

Nesse contexto, para que seja possível prover aplicações de múltiplos serviços NFC remotamente, é necessário um sistema de servidores que se comunicam com o dispositivo por rede móvel, composto pelo provedor de serviço, que seria o banco ou o emissor de serviço. [8]

Assim, esses cartões e aparelhos contam com um chip e uma antena de radiofrequência (RFID) integrados que permitem aos seus usuários realizarem uma transação sem fio com o terminal de pagamentos.

As especificações e os protocolos de comunicação não serão discutidos neste trabalho, pois não fazem parte de seu escopo, que busca o estudo do NFC e suas consequências jurídicas decorrentes da má utilização dessa tecnologia nas operações financeiras.

Os comerciantes gostam desse novo meio de pagamento porque as transações podem ser concluídas rapidamente, acelerando filas e aumentando as vendas. Como normalmente não é necessária nenhuma verificação de assinatura ou senha, as compras sem contato geralmente se limitam a vendas de pequeno valor.[9]

Os pesquisadores de segurança Leigh-Anne Galloway e Tim Yunusov alertam que "as vulnerabilidades nos pagamentos *contactless* representam uma ameaça à integridade do modelo de

[8] CRUZ, Kelly. *Estudo sobre o near field communication e seu papel em pagamentos via dispositivos móveis*. Trabalho apresentado no curso de pós-graduação em Rede de Computadores do Centro Universitário de Brasília - UniCEUB/ICPD, 2013.

[9] NOVAS vulnerabilidades na tecnologia Contactless - o chip é novo, mas a criptografia é antiga. *Madri*, 2019. Disponível em: <https://blog.midri.com.br/noticias/novas-vulnerabilidades-na-tecnologia-contactless/>. Acesso em: 18 de maio de 2020.

pagamento cada vez mais popular",[10] ambos afirmam que o protocolo criptográfico por trás dos pagamentos NFC é obsoleto e vulnerável.

3.1 Fraudes eletrônicas

A facilidade em pagar por aproximação oferecida pelos bancos por meio dos dispositivos móveis e cartões, tem gerado preocupação para os especialistas em tecnologia e segurança, bem como em seus clientes, posto que essa tecnologia está sendo aproveitada por pessoas especializadas em fraudes eletrônicas, situação que vem a confirmar a existência de insegurança nessas transações.

Dentre os delitos que ameaçam a comunicação entre dispositivos NFC, estão a escuta de dados, corrupção de dados, modificação de dados, inserção de dados e clonagem.

Tendo em vista que a transação ocorre rapidamente e que o limite não é alto para as transações que não necessitam de senha, muitos desses pagamentos por aproximação saem despercebidos, ainda mais porque grande maioria das pessoas não possuem o hábito de conferir seus extratos bancários diariamente.

Por essa razão, o NFC está sendo alvo de golpistas, que estão se aproveitando dessa tecnologia para a prática de furtos.[11] Os casos de roubo e golpes têm se tornado comuns e tendem a ser um problema ainda maior durante grandes eventos, como festas

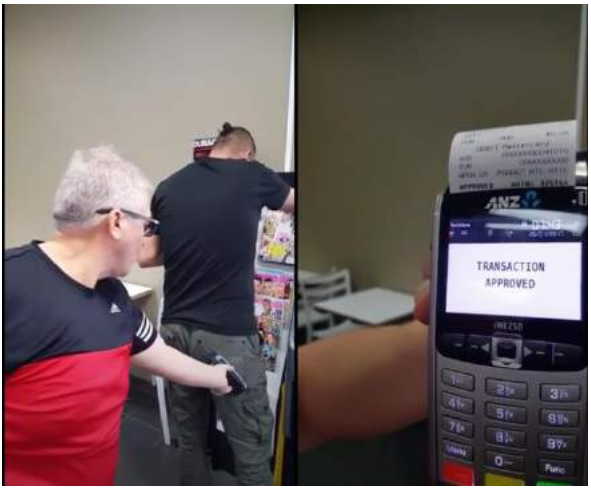
[10] GALLOWAY, Leigh-Anne; YUNUSOV, Tim; STENNIKOV, Aleksei. *First contact:* new vulnerabilities in contactless payments. 2019. Disponível em: <https://leigh-annegalloway.com/presentation-materials/>. Acesso em: 20 de maio de 2020.

[11] SILVA, Diony. Tecnologia que permite usar cartão por aproximação é alvo de golpistas; saiba como se proteger. G1 Globo, 2019. Disponível em: <https://g1.globo.com/es/espirito-santo/noticia/2019/08/21/tecnologia-que-permite-usar-cartao-por-aproximacao-e-alvo-de-golpistas-saiba-como-se-proteger.ghtml>. Acesso em: 18 de maio de 2020.

de shows e festas de carnaval, que possuem grande concentração de pessoas em um mesmo lugar, sendo mais fácil de aplicar fraudes.

Os criminosos, portando terminal para pagamento por aproximação, se valem da distração das vítimas para aproximar o leitor dos bolsos de suas calças, onde o cartão estaria guardado na carteira e, assim, obtendo a confirmação da transação.

Figura 1: Exemplo.



Fonte: Canal Nashagui do Youtube (2018)[12]

Os pagamentos *contactless* são muito convenientes, porém há duas maneiras que os dados de um cartão podem ser furtados. A primeira seria usando aplicativos para celular que permitem ler dados de cartão ou dispositivo sem contato e fazer transação bancária e a segunda seria utilizando um terminal ou maquineta para pagamentos por aproximação.

[12] HOW to steal money from your credit card with NFC. 2018. 1 Vídeo (5:25min). Publicado pelo canal Nashagui. Disponível em: < https://www.youtube.com/watch?v=VrreNp9Ebz8 >. Acesso em: 17 de maio de 2020.

Figura 2 - Pagamento com dispositivo móvel.

Fonte: Canal Blockr do Youtube (2018)[13]

Figura 3 - Pagamento com terminal.

Fonte: Canal Blockr do Youtube (2018)[14]

Assim, conclui-se que é fácil ser vítima de estelionato e consequentemente ter prejuízos financeiros, posto que os criminosos se valem de vários meios para aplicar as suas fraudes em desfavor da função *contactless*, de forma que o novo batedor de carteira pode ser um hacker passando ao seu lado em algum lugar movimentado como em uma rua, feira, ônibus ou metrô.

4 RESPONSABILIDADE DAS INSTITUIÇÕES BANCÁRIAS

No setor bancário, a vulnerabilidade decorrente dessa nova tecnologia está sendo alvo de interesse de hackers e organizações

[13] RFID Scanner Credit Card Theft - see how contactless credit cards have their details stolen. David Blockr, 2018. 1 Vídeo (3:15min). Publicado pelo canal Blockr. Disponível em: <https://www.youtube.com/watch?v=tIgUVrWRXMc>. Acesso em: 16 de maio de 2020.

[14] RFID Scanner Credit Card Theft - see how contactless credit cards have their details stolen. David Blockr, 2018. 1 Vídeo (3:15min). *Publicado pelo canal Blockr*. Disponível em: <https://www.youtube.com/watch?v=tIgUVrWRXMc>. Acesso em: 16 de maio de 2020.

criminosas, podendo comprometer a reputação de um banco e até levar a perda de confiança da tecnologia.[15]

Em razão da relação negocial bancária estabelecida entre os bancos e seus clientes, estes estão sujeitos às normas do Código de Defesa do Consumidor, eis que as instituições financeiras se enquadram no conceito de fornecedor de serviços e seus clientes como consumidor. Ao conceituar fornecedor e consumidor, os artigos 2º e 3º descrevem que:

> Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.
>
> Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo.[16]
>
> Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
>
> § 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial.
>
> § 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.[17]

---

[15] CRUZ, Kelly. *Estudo sobre o near field communication e seu papel em pagamentos via dispositivos móveis*. Trabalho apresentado no curso de pós-graduação em Rede de Computadores do Centro Universitário de Brasília - UniCEUB/ICPD, 2013.

[16] BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Código de Defesa do Consumidor. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 18 de maio de 2020.

[17] BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Código de Defesa do Consumidor. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 18 de maio de 2020.

A instituição bancária quando coloca determinados serviços à disposição do consumidor, se torna responsável por adotar os mecanismos de segurança cabíveis, a fim de evitar a ocorrência de possíveis fraudes, de forma que a responsabilidade pela falha na prestação de serviço é objetiva, nos termos do art. 14 do Código de Defesa do Consumidor.[18] Nesse contexto, a falta de segurança nos procedimentos adotados pelo banco, no que diz respeito às transações realizadas por meios eletrônicos, revela a inadequação e ineficiência dos serviços prestados.

Dessa forma, compete à instituição bancária, em face do risco inerente de sua atividade empresarial, dispor de meios tecnológicos seguros para provar a idoneidade das suas operações e evitar que ocorra a burla de seu sistema de segurança. Logo, em caso de fraude, o banco emissor do cartão é responsável por indenizar o consumidor quando o pagamento é feito sem senha.

5 CONCLUSÃO

O presente trabalho teve como objetivo analisar a tecnologia NFC, que possibilita o pagamento por aproximação, e as consequências jurídicas decorrentes da má utilização nas operações financeiras.

Diante do avanço das tecnologias, mudando cada vez mais os meios de pagamento no mundo, os meios eletrônicos são uma das formas mais utilizadas para pagamentos na atualidade, com destaque para os dispositivos móveis com a tecnologia contactless, sendo possível constatar como a evolução tecnológica tem

[18] BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Código de Defesa do Consumidor. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 18 de maio de 2020.

facilitado à vida das pessoas, tornando ações cotidianas, como por exemplo, o simples ato de pagar cada vez mais prático e rápido.

A tecnologia NFC e seu uso como um meio de pagamento se encontra em crescimento, chegando a ser mais rápida que uma transação convencional com chip ou tarja e mais rápido que o pagamento em dinheiro, agilizando o processo de pagamento e diminuindo filas nos estabelecimentos.

Os pagamentos por aproximação permitem que seus usuários reduzam a necessidade de usar o dinheiro, oferecendo comodidade, rapidez, desempenho e transferência de informações seguras entre os dispositivos a partir de uma transação simples em ambientes com alto volume de pagamentos, apresentando uma série de vantagens para as empresas e os consumidores que os utilizam.

Ademais, há medidas que podem ser adotadas pelos usuários para prevenir a fraude, como nunca colocar a carteira sobre a mesa ou no bolso de traseiro, bem como sempre bloquear o celular ao colocar na mesa ou no bolso. Outra forma de se proteger é desativar a funcionalidade de pagamento por NFC, contudo, perde-se a praticidade desse método.

REFERÊNCIAS

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Código de Defesa do Consumidor. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 18 de maio de 2020.

CRUZ, Kelly. *Estudo sobre o near field communication e seu papel em pagamentos via dispositivos móveis*. Trabalho apresentado no curso de pós-graduação em Rede de Computadores do Centro Universitário de Brasília - UniCEUB/ICPD, 2013.

GALLOWAY, Leigh-Anne; YUNUSOV, Tim; STENNIKOV, Aleksei. *First contact:* new vulnerabilities in contactless payments. 2019. Disponível em: <https://leigh-annegalloway.com/presentation-materials/>. Acesso em: 20 de maio de 2020.

HECKE, Caroline. Onde e como a tecnologia NFC está sendo aplicada. *Tecnomundo*, 2011. Disponível em: <https://www.tecmundo.com.br/nfc/8173-onde-e-como-a-tecnologia-nfc-esta-sendo-aplicada.htm>. Acesso em: 18 de maio de 2020.

HOW to steal money from your credit card with NFC. 2018. 1 Vídeo (5:25min). *Publicado pelo canal Nashagui*. Disponível em: < https://www.youtube.com/watch?v=VrreNp9Ebz8 >. Acesso em: 17 de maio de 2020.

NASSAR, Victor; VIEIRA, Milton L.H. *Método de Pesquisa para Análise da Experiência dos Usuários com a Tecnologia NFC (Near Field Communication)*. Universidade Federal de Santa Catarina, 2015. Disponível em: https://www.academia.edu/. Acesso em: 16 maio 2020.

NFC FORUM, 2013. Disponível em: <https://nfc-forum.org/>. Acesso em: 17 de maio de 2020.

NOVAS vulnerabilidades na tecnologia Contactless - o chip é novo, mas a criptografia é antiga. *Madri*, 2019. Disponível em: <https://blog.midri.com.br/noticias/novas-vulnerabilidades-na-tecnologia-contactless/>. Acesso em: 18 de maio de 2020.

RFID Scanner Credit Card Theft - see how contactless credit cards have their details stolen. David Blockr, 2018. 1 Vídeo (3:15min). *Publicado pelo canal Blockr*. Disponível em: <https://www.youtube.com/watch?v=tIgUVrWRXMc>. Acesso em: 16 de maio de 2020.

SILVA, Diony. Tecnologia que permite usar cartão por aproximação é alvo de golpistas; saiba como se proteger. *G1 Globo*, 2019. Disponível em: <https://g1.globo.com/es/espirito-santo/noticia/2019/08/21/tecnologia-que-permite-usar-cartao-por-aproximacao-e-alvo-de-golpistas-saiba-como-se-proteger.ghtml>. Acesso em: 18 de maio de 2020.

VASQUES, Victor. PagSeguro lança serviço de NFC no Brasil, para pagamentos via celular. *Techtudo*, 2012. Disponível em: <https://www.techtudo.com.br/artigos/noticia/2012/04/pagseguro

-lanca-servico-de-nfc-no-brasil-para-pagamentos-celular.html>. Acesso em: 16 de maio de 2020.

ENGENHARIA SOCIAL NA PANDEMIA DO NOVO CORONAVÍRUS

Gabriel Augusto Soares Seibel[1]

RESUMO

O presente trabalho, baseado na metodologia de pesquisa bibliográfica, estudará os casos de crimes virtuais praticados, por meio dos mecanismos enganosos das Fake News, durante o surto provocado pelo agente COVID-19 no Brasil. Os agentes delituosos aproveitando-se do uso de aplicativos que infectam os computadores e dispositivos móveis por meio de códigos maliciosos, igualmente conhecidos como pragas e malware, para o desaparecimento ou apropriação indevida de informações pessoais e profissionais acabam em razão deles apoderando-se de dados intransferíveis. Sem a pretensão de esgotar o tema, serão apontadas algumas das vulnerabilidades encontradas, meios de execução utilizados pelos criminosos, e a importância da adoção de medidas, para a diminuição desses tipos de golpes na internet. Ao fim, concluiremos com uma análise crítica e construtiva sobre o respectivo assunto.

Palavras-chave: Mecanismos. Informações. Golpes.

ABSTRACT

The present work, based on the bibliographic research methodology, will study the cases of virtual crimes committed, through the deceptive mechanisms of Fake News, during the

[1] Aluno da pós-graduação *lato sensu* em Direito Digital, Inovação e Tecnologia, pelo Instituto Ceub de Pesquisa e Desenvolvimento – ICPD/UniCEUB.

outbreak caused by the agent COVID-19 in Brazil. Criminal agents taking advantage of the use of applications that infect computers and mobile devices by means of malicious codes, also known as pests and malware, for the disappearance or misappropriation of personal and professional information end up by taking over data. non-transferable. Without intending to exhaust the topic, some of the vulnerabilities found, means of execution used by criminals, and the importance of adopting measures to reduce these types of scams on the Internet will be pointed out. At the end, we will conclude with a critical and constructive analysis on the respective subject.

Keywords: Mechanisms. Information. Scams.

1 INTRODUÇÃO

O sistema de saúde e econômico de muitos países, e sobretudo sua população, adoeceram perante uma cadeia de eventos suscitado pelo aparecimento de um novo vírus, identificado em 31 de dezembro de 2019 após a eclosão das primeiras vítimas na cidade de Wuhan, na província de Hubei, na China.

A doença infeciosa foi classificada pela Organização Mundial da Saúde (OMS) como COVID-19 causada pelo novo coronavírus (Sars-Cov-2). Decorridos apenas seis meses[2] da sua disseminação, as suas consequências são devastadoras: o número de infectados já ultrapassa os 6 milhões[3] em países diversificados, resultando em 360 mil[4] mortes até o momento. Fronteiras foram fechadas e severas políticas de distanciamento social têm sido implantadas na

[2] NOGUEIRA, Luiz. Covid-19: Brasil registra mais 33 mil infectados em 24 horas. Disponível em: <https://olhardigital.com.br/coronavirus/noticia/covid-19-brasil-supera-414-mil-casos-mortes-passam-de-25-mil/98089>. Acessado em: 30/05/2020.

[3] NOGUEIRA, Luiz. Covid-19: Brasil registra mais 33 mil infectados em 24 horas. Disponível em: <https://olhardigital.com.br/coronavirus/noticia/covid-19-brasil-supera-414-mil-casos-mortes-passam-de-25-mil/98089>. Acessado em: 30/05/2020.

[4] NOGUEIRA, Luiz. Covid-19: Brasil registra mais 33 mil infectados em 24 horas. Disponível em: <https://olhardigital.com.br/coronavirus/noticia/covid-19-brasil-supera-414-mil-casos-mortes-passam-de-25-mil/98089>. Acessado em: 30/05/2020.

tentativa de conter o avanço do vírus, que já mantém pelo menos mais de um terço[5] dos habitantes em quarentena ao redor do mundo. Na economia, revistas colocam para baixo as previsões de crescimento mundial de 2020, segundo o Fundo Monetário Internacional.

Diante dessa situação pandêmica, criminosos enxergaram uma perfeita oportunidade para novos golpes e desinformação: dispondo da notoriedade do assunto, dispersam áudios, vídeos e mensagens de textos com notícias falsas, no intuito de causar atribulações e para práticas delituosas, persuadindo suas vítimas para que acessem *links* fraudulentos que escondem ameaças invisíveis – os códigos maliciosos – para obtenção e modificação de dados sigilosos e sensíveis das vítimas, que serão usados em novos golpes.

Da mesma forma, passando-se por agentes de instituições oficiais, reclamam atualizações de dados bancários, planos de saúde etc., valendo-se da expansão da forma de trabalho *home office* amplamente utilizada em decorrência do isolamento social, sobredito, causando ainda mais pânico e incertezas sociais, prejudicando o funcionamento de muitos serviços essenciais que dependem dos sistemas de informação.

A proposta do estudo é debruçar-se sobre alguns dos mecanismos causadores e propagadores desta situação, a saber: os impactos das *Fake News* em um cenário pandêmico com o propósito de causar danos a terceiros bem como os golpes virtuais que têm sido aplicados e seu modo de execução, concluindo-se com os cuidados a serem observados para a identificação da má

[5] BRASIL, BBC NEWS. Coronavírus: um terço da população mundial está sob quarentena; veja 4 tipos de restrição. Disponível em: <https://www.bbc.com/portuguese/internacional-52040808>. Acessado em: 30/05/2020.

informação e diminuição do seu compartilhamento nas redes sociais, entre outras maneiras de ser prevenir.

2 AS NOTÍCIAS FALSAS SOBRE O NOVO CORONAVÍRUS COMO FONTE DE ENGENHARIA SOCIAL

O mundo já cedeu ao fascínio da internet. Ela propicia que seus usufruidores tenham acesso a imensuráveis possibilidades.

Todos os dias milhares informações e dados são transmitidos por meio de vídeos, imagens, áudios, mensagens de textos etc. que são compartilhados, armazenados, divididos e acessados. Também graças a essa tecnologia, com a modernização dos meios de comunicação em massa, em especial, através das mídias sociais, houve mudanças na maneira de pensar, agir e relacionar socialmente, refletidas nos mais diversos aspectos (p. ex., afetivos, jurídicos, acadêmicos, políticos e profissionais). Nenhuma outra civilização obteve meios de comunicação tão eficazes.

Porém, se a sociedade, em todo o tempo, conviveu com ameaças silenciosas que a colocaram em risco inclusive de extinção[6], não seria – e não é! – diferente agora. E, apesar da imensa quantidade de informação disponível a um simples clique, a verdade é que, no contexto virtual, a segurança da informação está sempre um (ou dois) passos atrás das ameaças e dos atacantes (*crackers*): a título de exemplo, pode-se observar recentemente um elevado número de invasões a dispositivos de autoridades públicas de primeiro e segundo escalão (Ministros de

[6] A título de exemplo, a peste negra evidenciou essa disparidade existente entre homens e agentes infecciosos sendo a causadora do desaparecimento de um terço da população europeia. Esse encolhimento populacional equivaleu ao decréscimo de 450 milhões para 350 milhões de indivíduos. Disponível em: <https://revistagalileu.globo.com/Ciencia/Saude/noticia/2020/03/conheca-5-maiores-pandemias-da-historia.html>. Acessado em: 28/05/2020.

Estado, Senadores, Deputados Federais...) do Brasil, conquanto as medidas de segurança tomadas e a proximidade aos órgãos de inteligência.

Outra grande ameaça nos tempos informáticos é a chamada engenharia social. Conceituada como a "técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações"[7] ou, em outras palavras, a "prática de má-fé usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes"[8]. Algumas práticas do gênero são copiosamente bem sucedidas apenas com o simples oferecimento de vantagens as suas vítimas, basta ver o golpe do site de comércio eletrônico fraudulento[9] em que o indivíduo aceita como verdadeiro o anúncio disponibilizado em um site gerado para não corresponder à realidade. A percepção do comprador de que se trata de uma tramoia é muitas vezes prejudicada pelo entusiasmo de conferir um preço extremamente convidativo. Geralmente, as vítimas desse tipo de golpe somente o percebem após efetuarem o pagamento ou em razão do não recebimento da mercadoria[10].

---

[7] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). *Cartilha Cert.Br – Glossário: Engenharia Social*. Disponível em: https://cartilha.cert.br/glossario/#e. Acessado em: 28/05/2020.

[8] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). Cartilha Cert.Br – Glossário: Engenharia Social. Disponível em: https://cartilha.cert.br/glossario/#e. Acessado em: 28/05/2020.

[9] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). *Cartilha Cert.Br – Golpes na internet: Golpe do site de comércio eletrônico fraudulento*. Disponível em: https://cartilha.cert.br/golpes/. Acessado em: 28/05/2020.

[10] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). *Cartilha Cert.Br – Golpes na internet: Golpe do site de comércio eletrônico fraudulento*. Disponível em: https://cartilha.cert.br/golpes/. Acessado em: 28/05/2020.

Uma prática criminosa que vem sendo abundantemente utilizada é a "sextorsão"[11]. O mais comum golpe consiste no envio de um e-mail contendo uma mensagem com a senha atual ou antiga e o nome completo da vítima. Os criminosos indicam estar sob a posse de vídeos ou imagens de suas vítimas que seriam oriundos dos vazamentos das câmeras dos seus aparelhos eletrônicos. E caso não ocorra a transferência de valores[12] preferencialmente em moeda virtual, haverá tão logo, a divulgação daquele material. Eis uma pequena amostra da engenharia social, objeto do presente trabalho.

A engenharia social é grande favorita dos golpistas por incidir sobre a maior vulnerabilidade existente: a humana. Independentemente de quantos recursos de segurança sejam utilizados, ou de sua eficácia, todos eles podem ser ultrapassados por um único usuário imprudente ou enganado. Vulnerabilidade esta que se amplia à medida da desinformação do usuário/vítima. Não por outro motivo, esse conhecimento é constantemente aplicado para a criação e divulgação de informações polêmicas, muitas vezes inverídicas, destinadas a provocar a atenção do leitor e, enfim, a prática de golpes pelas mídias sociais.

O telefone foi um dos primeiros instrumentos utilizados na aplicação de golpes servindo-se da engenharia social. Ele eternizou *Kevin Mitnick*[13], aquele que é considerado o maior cracker[14] de

[11] CAMBAÚVA, Fernanda Darcie;FARO, Jaqueline de Ramos Ribeiro. "Sextorsão": quanto custa a sua intimidade? Disponível em: <https://www.conjur.com.br/2020-mai-18/opiniao-sextorsao-quanto-custa-intimidade>. Acessado em: 28/05/2020.

[12] CAMBAÚVA, Fernanda Darcie; FARO, Jaqueline de Ramos Ribeiro. "Sextorsão": quanto custa a sua intimidade? Disponível em: <https://www.conjur.com.br/2020-mai-18/opiniao-sextorsao-quanto-custa-intimidade>. Acessado em: 28/05/2020.

[13] FONSECA, Willian. Quem é Kevin Mitnick? Disponível em: <https://www.tecmundo.com.br/historia/1842-quem-e-kevin-mitnick-.htm>. Acessado em: 29/05/2020.

todos os tempos, por invadir sistemas telefônicos e utilizá-los para realização desses golpes. O uso do telefone, melhor dizendo, das ligações telefônicas ainda está entre os meios mais estimados pelos criminosos. Isso se dá em razão da preservação do anonimato e pela simplicidade em abusar da intimidade da vítima, confundindo-a apenas com o uso de dados sensíveis.

E na pandemia do novo coronavírus não poderia ser diferente. Sabe-se por exemplo que alguém se passando por um funcionário de um hospital particular e com informações privilegiadas de uma paciente de 56 anos diagnosticada com a doença do Covid-19, entrou em contato com uma família alegando, que ela necessitava o quanto antes da assistência de aparelhos, medicamentos e exames não cobertos pelo plano de saúde[15]. O criminoso recorrendo da engenharia social para o convencimento da vítima, alegava veementemente que caso assim não fosse feito, o quadro de saúde daquela pessoa que estava acometida pelo novo coronavírus poderia apresentar sintomas ou avançar para um caso mais grave de câncer. "Aguardar o plano, é deixar o câncer evoluir."[16] Dizia ele, foi feita a transferência bancária da vítima para o golpista no valor de R$ 7.000 reais. Quando na verdade tudo se encaminhou para a confirmação de mais um golpe.

---

[14] FONSECA, Willian. Quem é Kevin Mitnick? Disponível em: <https://www.tecmundo.com.br/historia/1842-quem-e-kevin-mitnick-.htm>. Acessado em: 29/05/2020.

[15] BRASIL, Correio Braziliense. Covid-19: família cai em golpe após suposto funcionário pedir R$ 7 mil. Disponível em: >https://www.correiobraziliense.com.br/app/noticia/brasil/2020/05/27/interna-brasil,858639/covid-19-familia-cai-em-golpe-apos-suposto-funcionario-pedir-r-7-mil.shtml>. Acessado em: 28/05/2020.

[16] BRASIL, Correio Braziliense. Covid-19: família cai em golpe após suposto funcionário pedir R$ 7 mil. Disponível em: >https://www.correiobraziliense.com.br/app/noticia/brasil/2020/05/27/interna-brasil,858639/covid-19-familia-cai-em-golpe-apos-suposto-funcionario-pedir-r-7-mil.shtml>. Acessado em: 28/05/2020.

Sendo assim, não é difícil entender o porquê uma infinidade de golpes baseados na pandemia do Covid-19 tem surgido, valendo-se do pânico causado pelo grande número de mortes ao redor do mundo sem que se tenha uma possibilidade concreta de saída. É apenas mais um meio, canal, a "bola da vez"; amanhã serão outros. A combinação entre engenharia social e *softwares* maléficos corrobora ainda mais para a camuflagem dos golpes. O programa aplicativo intitulado de COVID-19tracker[17] que aparentemente declarava transmitir as últimas averiguações sobre os avançamentos do novo coronavírus em circunstâncias globais. É um exemplo disso, já que bem diferente do que prometerá, esse *app* encobria um plano bem mais audacioso. Ele nada mais é do que um *malware* conhecido como *Ransoware*[18], que depois de posto e executado no dispositivo móvel da vítima, criptografa e interrompe as suas finalidades habituais. Em seguida, exige como forma de extorsão o pagamento em moeda Bitcoin[19] pela liberação dos dispositivos infectados.[20] A vítima se vê no auge da impotência uma vez que não há garantia alguma, ainda que viesse a realizar todas as exigências dos golpistas de que tenha todos os seus dados e acessos devolvidos.

---

[17] PINHEIRO, Mirelle. Coronavírus: criminosos criam falso app e aplicam golpes na web. Disponível em: >https://www.metropoles.com/distrito-federal/coronavirus-criminosos-criam-falso-app-e-aplicam-golpes-na-web>. Acessado em: 28/05/2020.

[18] PINHEIRO, Mirelle. Coronavírus: criminosos criam falso app e aplicam golpes na web. Disponível em: <https://www.metropoles.com/distrito-federal/coronavirus-criminosos-criam-falso-app-e-aplicam-golpes-na-web>. Acessado em: 28/05/2020.

[19] PINHEIRO, Mirelle. Coronavírus: criminosos criam falso app e aplicam golpes na web. Disponível em: <https://www.metropoles.com/distrito-federal/coronavirus-criminosos-criam-falso-app-e-aplicam-golpes-na-web>. Acessado em: 28/05/2020.

[20] PINHEIRO, Mirelle. Coronavírus: criminosos criam falso app e aplicam golpes na web. Disponível em: <https://www.metropoles.com/distrito-federal/coronavirus-criminosos-criam-falso-app-e-aplicam-golpes-na-web>. Acessado em: 28/05/2020.

Bem como é possível perceber a preferência da utilização das redes sociais como meios de propagação através do seu alcance: segundo relatório de empresas de dados americanas – a *Hootsuite* e a *We Are Social* –, estimou-se que 3,5 bilhões de pessoas estivessem cadastradas em alguma rede social já em 2019.[21] Uníssono, a empresa *Google LLC*, responsável pela plataforma de *webmail "Gmail",* afirmou, recentemente, ter detectado uma média de 18 milhões de e-mails disparados diariamente contendo *malwares* ou servindo de iscas para atração de vítimas para ataques via web (*phishing*) valendo-se de notícias relacionadas à pandemia.[22]

No Brasil, essas notícias estão espalhadas pelas principais plataformas digitais – *Facebook*, *Instragram*, *Twitter*, *Youtube* e *Whatsapp –,* disseminando as mais variadas inverdades somente com os golpes envolvendo o novo coronavírus. Nesta última (*Whatsapp*), estima-se que potenciais golpes lastreados no Covid-19 ultrapassaram os 11 milhões de acessos e compartilhamentos,[23] contando com a agravante da incapacidade

[21] Informação divulgada em seu relatório conjunto *Global Digital Statshot 2019. Disponível em:* <https://super.abril.com.br/tecnologia/metade-do-planeta-esta-nas-redes-sociais-que-ja-somam-35-bilhoes-de-usuarios/>. Acessado em: 24/05/2020.

[22] O Google afirmou ter detectado 18 milhões de mensagens por dia de malware e phishing no Gmail relacionadas à pandemia. "Uma campanha notável tentou direcionar contas pessoais de funcionários do governo dos EUA com iscas de phishing usando redes norte-americanas de fast food e mensagens sobre Covid-19. Disponível em: <https://forbes.com.br/colunas/2020/04/google-diz-que-hackers-apoiados-por-governos-estao-intensificando-ataques-de-phishing/>. Acessado em 24/05/2020.

[23] REIS, Emanuel. Golpes sobre Covid-19 no WhatsApp têm 11 milhões de acessos e envios. Disponível em: <https://www.techtudo.com.br/noticias/2020/05/golpes-sobre-covid-19-no-whatsapp-tem-11-milhoes-de-acessos-e-envios.ghtml>. Acessado em: 24/05/2020.

da maioria dos brasileiros em distinguir as notícias falsas (*Fake News*) das verdadeiras.[24]

Entre elas, estão o falso programa auxilio cidadão, distribuição gratuita de álcool em gel pela Ambev em todas as cidades do país, Netflix liberada e o Voucher da Heineken que consistiam em dar privilégios e serviços gratuitos para aqueles que estavam impelidos pelo Covid-19 ao isolamento social, mas que, na verdade, escondiam conteúdo falso para o roubo de dados por meio de *phishing*.

Ainda sobre, de acordo com a empresa *Kaspersky Lab*, prestadora de serviços de segurança na internet por meio de softwares,

> Ataques phishing contra dispositivos móveis mais que dobraram no último mês no Brasil, aponta levantamento da Kaspersky. De fevereiro a março, detectamos aumento de 124% neste tipo de golpe – crescimento diretamente ligado às mensagens maliciosas circulando no WhatsApp se aproveitando da pandemia. Entre as principais formas utilizadas para ganhar dinheiro, essas mensagens fazem a vítima baixar apps legítimos (sendo remunerado via programas de afiliação) ou roubam os dados pessoais do usuário para usá-los em outros ataques.[25]

Portanto, conclui-se a importância da informação para a profilaxia das doenças humanas e virtuais, uma vez que, assim como uma medicina capaz de diagnosticar e medicar com eficiência evita maiores danos à saúde da população, um

[24] A empresa Kasperky que presta serviços de segurança na internet por meio de softwares realizou um estudo "Iceberg digital" juntamente com a empresa de pesquisa CORPA, na América Latina conclui que 62% dos brasileiros não conseguem reconhecer uma notícia falsa Disponível em: <https://canaltech.com.br/seguranca/brasileiros-nao-sabem-reconhecer-fake-news-diz-pesquisa-160415/>. Acessado em: 24/05/2020.

[25] RODRIGUES, Renato. Ataques a dispositivos móveis crescem 124% em março. Disponível em: <https://www.kaspersky.com.br/blog/phishing-covid-smartphone-pesquisa/14663/>. Acessado em: 28/05/2020.

cidadão/usuário bem informado tem melhores condições de filtrar aquilo que é potencialmente falso, deixando de repassar e buscando fontes seguras para a checagem dos fatos, evitando-se golpes na internet.

3 ASPECTOS JURÍDICOS DAS FAKE NEWS NA PANDEMIA DO NOVO CORONAVÍRUS

Sobrou engenhosidade nessa pandemia do novo coronavírus para a invenção e lançamento de notícias falsas. Qualquer ser humano conectado à internet pode vir a se tornar um potencial disseminador de conteúdo falso. Afinal, é da nossa natureza supormos muitos fatos e quando percebemos inconscientemente, já estamos construindo e repassando várias crenças trasvestidas de informações. Talvez seja, esse o caso do ensinamento que costumávamos ouvirmos dos nossos pais que poderíamos contrair uma gripe ou resfriado apenas pelo fato de ter ficarmos expostos a chuva ou ao frio demasiadamente – como é sabido o que provoca doenças são os vírus[26] e não as baixas temperaturas.

O problema se torna mais grave quando esses casos envolvem os geradores de opiniões contemporâneos tais como influenciadores digitais, seguidos de políticos, celebridades e figuras públicas e assim por diante, que abastecem publicamente as redes sociais quer seja intencional ou não a ponto de ultrapassar as barreiras da legalidade por espalharem vertiginosamente acontecimentos ilegítimos capazes de promover uma série de prejuízos. Lastimavelmente muitos crimes contra a honra ainda não são solucionados ou por falta de investigação efetiva do Estado ou pelo próprio desinteresse da vítima e o

[26] PRADO, Ana Carolina. Pegar friagem provoca resfriado? Disponível em: <https://super.abril.com.br/saude/pegar-friagem-provoca-resfriado/>. Acessado em: 30/05/2020.

desfecho dessa omissão quase sempre é a impossibilidade de atingir a autoria delitiva, permitindo que não se alcance a justiça. Independentemente de as redes sociais serem um ambiente favorável a comunicação engana-se aquele que acredita que pode divulgar o que lhe convém.

Expressamente o simples ato de divulgar *fakes news* ainda necessita de uma melhor regulamentação para que seja considerado crime. Isso não significa que a legislação penal brasileira não preveja em sua baila delitos que aludem a produção de notícia falsas, especialmente na lei de crimes financeiros, de falências, e no nosso código eleitoral do Brasil dentre outros.

Nesse sentido, é destinada a proposta do deputado federal Luiz Carlos Hauly pretende tipificar penalmente as Fake News, através do artigo 1º caput do Projeto de Lei nº 6.812/17, como o ato de "divulgar ou compartilhar, por qualquer meio, na rede mundial de computadores, informação falsa ou prejudicialmente incompleta em detrimento de pessoa física ou jurídica".[27] Caminha com mesmo propósito ou equivalente, o Projeto de Lei nº 473/17, de autoria do Senador Ciro Nogueira, para que inclua a tipificação no código penal brasileiro do Art. 287-A, in verbis: "divulgar notícia que sabe ser falsa e que possa distorcer, alterar ou corromper a verdade sobre informações relacionadas à saúde, à segurança pública, à economia nacional, ao processo eleitoral ou que afetem interesse público relevante".[28] Atualmente com a exuberância dos crimes contra a honra na internet a se saber a "falsa imputação de

[27] BRASIL. Projeto de Lei nº 6.812 de 2017. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1522471&filename=PL+6812/2017>. Acesso em: 27/05/2020.

[28] BRASIL. Projeto de Lei nº 473 de 2017. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7312821&disposition=inline>. Acessado em: 27/05/2020.

crime (calúnia)"[29], "a imputação de fatos ofensivos à reputação (difamação)"[30] "e a ofensa à dignidade ou ao decoro (injúria)"[31] foram banalizadas e que ao se buscar as medidas judiciais cabíveis a sensação é de impunidade.

Essas notícias falsas vêm causando inúmeros transtornos ao meio jurídico e jornalístico e desassossega o nosso já pressionado panorama político atual. Toda essa atemorização vivida no Brasil não é coisa exagerada visto que neste momento ocupamos a **segunda colocação entre os países no planeta** com maior quantidade de casos validados do covid-19, só perde para os Estados Unidos[32]. Os brasileiros tiveram com essa calamidade o cômputo de **27.944**[33] **vidas encurtadas e os números vão aumentando a cada dia.** Nesse decurso, não seria nenhum absurdo que em breve seja ventilado a possibilidade do surgimento de uma legislação específica que decida como transgressão de uma lei a elaboração e a disseminação de *Fake News* que ameaçam à saúde coletiva em épocas pandêmicas. Ainda bem que catástrofes biológicas como essa embora sejam assustadoras são deveras incomuns.

[29] BRASIL, Código Penal Brasileiro. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acessado em 29/05/2020.

[30] BRASIL, Código Penal Brasileiro. Disponível em: >http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acessado em 29/05/2020.

[31] BRASIL, Código Penal Brasileiro. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acessado em 29/05/2020.

[32] G1, Portal de Notícias. Casos de coronavírus e número de mortes no Brasil em 29 de maio. Disponível em: <https://g1.globo.com/bemestar/coronavirus/noticia/2020/05/29/casos-de-coronavirus-e-numero-de-mortes-no-brasil-em-29-de-maio.ghtml>. Acessado em: 30/05/2020.

[33] G1, portal de notícias. Casos de coronavírus e número de mortes no Brasil em 29 de maio. Disponível em: <https://g1.globo.com/bemestar/coronavirus/noticia/2020/05/29/casos-de-coronavirus-e-numero-de-mortes-no-brasil-em-29-de-maio.ghtml>. Acessado em: 30/05/2020.

Uma pesquisa pormenorizada pelo Centro de Estudos e Pesquisas de Direito Sanitário (Cepedisa) da USP, em junção com o Centro de Análise da Liberdade e do Autoritarismo (LAUT) e do Instituto Nacional de Ciência e Tecnologia em Democracia Digital (INCT.DD), da Universidade Federal da Bahia.[34] Disponibilizou um ensaio denominado **Ciência Contaminada - Analisando o Contágio de Desinformação Sobre Coronavírus via *YouTube***, nele foi permitido aperceber que,

> O trabalho foi realizado em duas fases. A primeira analisou 11.546 vídeos entre 1º de fevereiro e 17 de março. A segunda acompanhou 12.775 produções entre 18 de março e 1º de maio. No total, o grupo identificou que vídeos com desinformação sobre a COVID-19 tiveram 73,4 milhões de visualizações contra apenas 27,7 milhões de visualizações de canais com produções de notícias verdadeiras.[35]

Averiguou-se mediante a apresentação de resultados que os internautas estão possuindo uma maior preferência pela busca de vídeos verdadeiramente falsos pela plataforma do *Youtube* em relação a aqueles que continham informações verídicas.

São notícias estruturadas para atrair um determinado público com títulos expressivos e sensacionalistas. Esse grupo de pessoas pode ser constituído de indivíduos com baixa ou nenhuma escolaridade[36] que recorrem cada vez mais para as redes sociais para promoverem o seu conhecimento. Em consequência também,

---

[34] WAKKA, Wagner. No YouTube, divulgação de vídeos fakes é 3 vezes maior que os verdadeiros. Disponível em: >https://canaltech.com.br/internet/no-youtube-divulgacao-de-videos-fakes-e-3-vezes-maior-que-os-verdadeiros-165234/>. Acessado em: 28/05/2020.

[35] WAKKA, Wagner. No YouTube, divulgação de vídeos fakes é 3 vezes maior que os verdadeiros. Disponível em: >https://canaltech.com.br/internet/no-youtube-divulgacao-de-videos-fakes-e-3-vezes-maior-que-os-verdadeiros-165234/>. Acessado em: 28/05/2020.

[36] CAMPOS, Lorraine Vilela. O que são Fake News? *Brasil Escola*. Disponível em: < https://brasilescola.uol.com.br/curiosidades/o-que-sao-fake-news.htm>. Acessado em: 30/05/2020.

do aperfeiçoamento da tecnologia do aparelho celular que permitiu que ele pudesse realizar quase as mesmas serventias de um computador doméstico e por um valor bem mais acessível. Tornando-o o seu cada vez mais popular.

Equivocar-se quem pensa que apenas eles estão sendo apanhados pelas notícias falsas. Há indivíduos com maior grau de escolaridade sendo persuadidos por essas mentiras que transformam as informações dos seus candidatos políticos para parecerem cada vez mais atraentes ou dignos de impopularidade.[37] A medida que os compartilhamentos de uma notícia falsa vão se tornando virais ela vai dando a impressão de que é sim uma informação confiável. E as consequências podem ser desastrosas.

Que bom que com simples precauções é possível manter uma navegação mais segura e evitar alguns golpes. É importante variar as senhas periodicamente e não as repetir para todos os acessos. Se possível não as memorize no navegador já que podem ser sim resgatadas. Os *links*, *spam* e *downloads* podem encobrir objetivos prejudiciais, em todo o caso é aconselhável averiguar a sua procedência. As informações duvidosas podem com facilidade de serem certificadas quanto ao que está em seu teor. Para tanto, há sites que desmascaram se uma notícia é falsa ou verdadeira, isso é realizado gratuitamente.[38] É sabido que elas são muito convenientes para alguns e podem representar uma ocupação extraordinariamente rendosa. Não é exaustivo lembrar que para que alguém venha a triunfar o outro tenha que sair derrotado. Na dúvida jamais divulgue!

---

[37] CAMPOS, Lorraine Vilela. O que são Fake News? *Brasil Escola*. Disponível em: < https://brasilescola.uol.com.br/curiosidades/o-que-sao-fake-news.htm>. Acessado em: 30/05/2020.

[38] COSTA, Matheus Bigogno. 5 sites para checar se a notícia é verdadeira ou falsa. Disponível em: <https://canaltech.com.br/internet/sites-para-checar-noticia-verdadeira-ou-fake-news/>. Acessado em: 30/05/2020.

4 CONCLUSÃO

Ainda não se sabe quantos meses mais a pandemia do novo coronavírus no Brasil vigorará. Fato é que o falso noticiário posto em atividade através das *fakes news* na era da tecnologia certamente não vai deixar de ser continuado. Os criminosos irão acompanhar as mais recentes tramas sociais para que possam contribuir com um melhor desempenho das táticas persuasivas. Afinal de contas, a má conduta de não dizer a verdade, nenhuma vez mudou com o passar dos anos, mas sim as circunstâncias, meios e os fins.

A penalização das *fake news* apesar de ser considerável esbarra em algumas incertezas jurídicas. Diz-se isso, pois concebeu-se que esse termo é de certo modo demasiado genérico, sem que houvesse um consenso internacional ou sequer local, acarretar a criação de um tipo penal seria o mesmo que "*tapar o sol* com a *peneira*" que, ora pode vir a permitir abusos estatais, ora omissões, dado a não conseguir delimitar as condutas que visa punir, tornando-se ineficaz na prática. Ademais, questiona-se se essa tipificação apressada não ofenderia o exercício do direito de liberdade de expressão e de imprensa, uma vez que pode resultar na remoção de conteúdo inteiramente verdadeiro.

Destarte, o direito penal não deve ser constantemente acionado e aplicado a todos os males que assolam a sociedade, pressionando o legislador a editar normas de interpretações equivocadas como ocorre, ou poderia ocorrer no caso das *fake news*. Por mais bizarra que uma notícia possa se apresentar, a sua verdade merece ser revelada.

REFERÊNCIAS

BRASIL, BBC NEWS. Coronavírus: um terço da população mundial está sob quarentena; veja 4 tipos de restrição. Disponível em: <https://www.bbc.com/portuguese/internacional-52040808>. Acessado em: 30/05/2020.

BRASIL, Código Penal Brasileiro. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acessado em 29/05/2020.

BRASIL, Correio Braziliense. Covid-19: família cai em golpe após suposto funcionário pedir R$ 7 mil. Disponível em: >https://www.correiobraziliense.com.br/app/noticia/brasil/2020/05/27/interna-brasil,858639/covid-19-familia-cai-em-golpe-apos-suposto-funcionario-pedir-r-7-mil.shtml>. Acessado em: 28/05/2020.

BRASIL. Projeto de Lei nº 473 de 2017. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7312821&disposition=inline>. Acessado em: 27/05/2020.

BRASIL. Projeto de Lei nº 6.812 de 2017. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1522471&filename=PL+6812/2017>. Acesso em: 27/05/2020.

CAMBAÚVA, Fernanda Darcie; FARO, Jaqueline de Ramos Ribeiro. "Sextorsão": quanto custa a sua intimidade? Disponível em: <https://www.conjur.com.br/2020-mai-18/opiniao-sextorsao-quanto-custa-intimidade>. Acessado em: 28/05/2020.

CAMPOS, Lorraine Vilela. O que são Fake News? *Brasil Escola*. Disponível em: <https://brasilescola.uol.com.br/curiosidades/o-que-sao-fake-news.htm>. Acessado em: 30/05/2020.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). *Cartilha Cert.Br – Glossário: Engenharia Social*. Disponível em: https://cartilha.cert.br/glossario/#e. Acessado em: 28/05/2020.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). *Cartilha Cert.Br – Golpes na internet: Golpe do site de comércio eletrônico fraudulento*.

Disponível em: https://cartilha.cert.br/golpes/. Acessado em: 28/05/2020.

COSTA, Matheus Bigogno. 5 sites para checar se a notícia é verdadeira ou falsa. Disponível em: < https://canaltech.com.br/internet/sites-para-checar-noticia-verdadeira-ou-fake-news/>. Acessado em: 30/05/2020.

FONSECA, Willian. Quem é Kevin Mitnick? Disponível em: <https://www.tecmundo.com.br/historia/1842-quem-e-kevin-mitnick-.htm>. Acessado em: 29/05/2020.

G1, Portal de Notícias. Casos de coronavírus e número de mortes no Brasil em 29 de maio. Disponível em: <https://g1.globo.com/bemestar/coronavirus/noticia/2020/05/29/casos-de-coronavirus-e-numero-de-mortes-no-brasil-em-29-de-maio.ghtml>. Acessado em: 30/05/2020.

NOGUEIRA, Luiz. Covid-19: Brasil registra mais 33 mil infectados em 24 horas. Disponível em: <https://olhardigital.com.br/coronavirus/noticia/covid-19-brasil-supera-414-mil-casos-mortes-passam-de-25-mil/98089>. Acessado em: 30/05/2020.

PINHEIRO, Mirelle. Coronavírus: criminosos criam falso app e aplicam golpes na web. Disponível em: >https://www.metropoles.com/distrito-federal/coronavirus-criminosos-criam-falso-app-e-aplicam-golpes-na-web>. Acessado em: 28/05/2020.

PRADO, Ana Carolina. Pegar friagem provoca resfriado? Disponível em: <https://super.abril.com.br/saude/pegar-friagem-provoca-resfriado/>. Acessado em: 30/05/2020.

REIS, Emanuel. Golpes sobre Covid-19 no WhatsApp têm 11 milhões de acessos e envios. Disponível em: <https://www.techtudo.com.br/noticias/2020/05/golpes-sobre-covid-19-no-whatsapp-tem-11-milhoes-de-acessos-e-envios.ghtml>. Acessado em: 24/05/2020.

WAKKA, Wagner. No YouTube, divulgação de vídeos fakes é 3 vezes maior que os verdadeiros. Disponível em: >https://canaltech.com.br/internet/no-youtube-divulgacao-de-videos-fakes-e-3-vezes-maior-que-os-verdadeiros-165234/>. Acessado em: 28/05/2020.

AGENTE INFILTRADO VIRTUAL: BREVES CONSIDERAÇÕES À LUZ DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE E DA LEI DE

Gabriella Emilia Ferreira Batista[1]

RESUMO

O agente infiltrado virtual foi introduzido no ordenamento jurídico pela Lei nº 13.441/2017 que alterou o Estatuto da Criança e do Adolescente. Em 2019, por meio do denominado "Pacote Anticrime", a Lei nº 12.850/2013 também passou a regular o tema, agora relacionado aos crimes envolvendo ou praticados por organização criminosa. O presente estudo, por meio da análise legislativa e bibliográfica, pretende expor as principais características e requisitos da infiltração virtual, bem como questões práticas atinentes a esta técnica de investigação.

Palavras-chave: Agente infiltrado virtual. Estatuto da Criança e do Adolescente. Lei de Organização Criminosa.

ABSTRACT

The virtual infiltrated agent was introduced into the legal system by Law No. 13.441/2017, which amended the Statute of Children and Adolescents. In 2019, through the so-called "Anticrime Package", the Law No. 12.850/2013 also started to regulate the theme regarding crimes involving or committed by a criminal organization. This study, by means of legislative and

[1] Bacharel em Direito pelo Centro Universitário de Brasília – UniCEUB. Aluna da pós graduação *lato sensu* em Direito Penal e Controle Social pelo UniCEUB. Aluna da pós graduação *lato sensu* em Direito Processual Civil pelo Centro Universitário UDF. E-mail: gabriellafbatista@gmail.com.

bibliographic analysis, intends to expose the main characteristics and requirements of virtual infiltration, as well as practical issues related to this investigation technique.

Keywords: Virtual infiltrated agent. Child and Adolescent Statute. Criminal Organization Law.

1 INTRODUÇÃO

Além de benefícios, o avanço tecnológico também trouxe preocupações. Hoje a comunicação entre as pessoas é facilitada por meio de aplicativos de conversação instantânea e pelas redes sociais. Da mesma forma, operações bancárias e compras pela internet são cada vez mais comuns.

De igual modo, o desenvolvimento dos meios digitais possibilitou o surgimento de novas modalidades de crimes, que buscam a obtenção de dados pessoais dos usuários ou que, utilizando o meio digital, praticam as infrações já previstas na legislação e conhecidas pela população. Por essa razão, as técnicas de investigação também tiveram que se aperfeiçoar.

Hoje é possível obter diversos dados nas denominadas fontes abertas, com acesso livre aos usuários. Porém, nem sempre as informações disponíveis serão suficientes para o crime que se investiga.

Assim, a legislação relativa à organização criminosa e aos crimes cometidos contra crianças e adolescentes passou a regular a aplicação da técnica investigativa do agente infiltrado virtual para os crimes contra a dignidade sexual da criança e do adolescente e para crimes praticados ou que envolvam organização criminosa.

Apesar de a infiltração de agentes não ser novidade, a regulamentação desse instituto nos meios virtuais é recente no direito brasileiro.

Assim, além de entender sobre os crimes cibernéticos, bem como as formas de investigação (em fontes abertas e fechadas), também serão abordadas questões práticas relativas à infiltração de agentes nos meios digitais.

Vale destacar que esse estudo não pretende esgotar os assuntos relativos ao tema, mas apresentar um panorama geral a partir das recentes alterações legislativas a respeito da infiltração virtual de agente.

2 CRIME PRÓPRIO E IMPRÓPRIO NO MEIO VIRTUAL

Os crimes digitais podem ser entendidos como condutas perpetradas em face de um sistema informático ou praticados contra outros bens jurídicos tutelados, utilizando-se da internet como meio para a prática de crime.[2]

É possível encontrar diversas classificações para os crimes cibernéticos, porém, para este estudo, adotar-se-á a classificação majoritária que divide os crimes digitais em próprios (ou puros) e impróprios (ou impuros).

Nos crimes digitais próprios os bens jurídicos atingidos são os sistemas informáticos, de telecomunicação ou de dados, portanto, protege-se a inviolabilidade dos dados.[3] Desse modo, o agente,

[2] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet**. São Paulo: Brasport, 2016, p. 35.
CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011, p. 66.

[3] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011, p. 67.

utilizando-se de meio informático, busca a obtenção de uma informação da vítima, por exemplo um dado bancário. Ou, o agente utiliza-se de um *spyware* – termo genérico para designar arquivos espiões – a fim de rastrear informações do usuário contidas no computador.

São exemplos de crimes próprios previstos no Código Penal a invasão de dispositivo informático (art. 154-A, CP), a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (art. 266, CP), a inserção de dados falsos em sistema de informações (art. 313-A, CP), dentre outros.[4]

Os crimes digitais impróprios são aqueles em que o agente se utiliza dos meios informáticos para a prática de crimes tipificados no ordenamento jurídico, os meios virtuais são, portanto, instrumentos para execução do delito. Nesse caso, não há ofensa ao bem jurídico da inviolabilidade da informação automatizada.[5]

Os exemplos mais comuns são os crimes de estelionato, calúnia, difamação, injúria, ameaça, induzimento instigação ou auxílio ao suicídio, divulgação de segredo, dentre outros.[6]

Ao discorrer sobre o tema, Alessandro Gonçalves Barreto e Beatriz Silveira Brasil, citando Norton Symantec, apresentam as principais características de ambas as modalidades[7]:

KUNRATH, Josefa Cristina Tomaz Martins**. A expansão da criminalidade no cyberespaço.** Feira de Santana: Universidade Estadual de Feira de Santana, 2017, p. 50.

[4] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet**. São Paulo: Brasport, 2016, p. 37/38.

[5] KUNRATH, Josefa Cristina Tomaz Martins**. A expansão da criminalidade no cyberespaço.** Feira de Santana: Universidade Estadual de Feira de Santana, 2017, p. 49.

[6] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet**. São Paulo: Brasport, 2016, p. 39/41.

Crime Digital Próprio	Crime Digital Impróprio
Normalmente acontece somente uma vez.	Interações repetidas com a vítima, visando aproveitar-se da relação para o cometimento do delito.
Geralmente é facilitado por softwares de atividades ilegais.	Normalmente utilizam-se de programas classificados como de atividades legais, como aplicativos de conversação instantânea.
Na maioria das vezes aproveita-se de falhas ou vulnerabilidades de segurança.	

3 INVESTIGAÇÕES EM FONTES ABERTAS E O AGENTE INFILTRADO VIRTUAL

3.1 Fontes abertas

Entende-se por fontes abertas aquelas a que se tem livre acesso, sem obstáculo à obtenção de dados e conhecimento.[8]

A título exemplificativo, a Lei de Acesso à Informação Pública (Lei nº 12.527/2011) estabelece uma série de procedimentos destinados a assegurar o direito fundamental de acesso à informação, como: a) observância da publicidade como preceito geral e do sigilo como exceção, b) divulgação de informações de interesse público, independente de solicitações, c) utilização de meios de comunicação viabilizados pela tecnologia da informação, d) fomento ao desenvolvimento da cultura de transparência na

[7] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet**. São Paulo: Brasport, 2016, p. 37/39.

[8] BARRETO, Alessandro Gonçalves; WENDT, Emerson**. Inteligência Digital:** *uma análise das fontes abertas na produção de conhecimento e de provas em investigações e processos*. Rio de Janeiro: Brasport, 2017, p. 6.

administração pública e, e) desenvolvimento do controle social da administração pública.[9]

Nesse sentido, os portais disponibilizados pelos órgãos estatais são um exemplo de fontes abertas, assim como aplicativos de conversação instantânea e redes sociais.

As fontes fechadas são aquelas cujos dados são protegidos (necessitando de credenciamento para acesso) ou negados (precisa de uma operação de busca para sua obtenção).[10]

Como exemplo de rede fechada temos a *deep web*, utilizada por muitos usuários como instrumento de compartilhamento de experiências criminosas, principalmente pelo caráter de anonimato que esse meio proporciona.[11]

Assim, para acessar redes fechadas é preciso que haja um convite ou a conquista da confiança de usuários. É nesse momento que será necessária a atuação do agente infiltrado virtual.[12]

A pesquisa em fontes abertas pode se revelar um ótimo instrumento de investigação. Porém, é necessário distinguir informação das denominadas *fake news* (notícias falsas).

---

[9] BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 30 maio 2020.

[10] BARRETO, Alessandro Gonçalves; WENDT, Emerson**. Inteligência Digital:** *uma análise das fontes abertas na produção de conhecimento e de provas em investigações e processos*. Rio de Janeiro: Brasport, 2017. Disponível em: <http://direitoeti.com.br/artigos/utilizacao-de-fontes-abertas-na-investigacao-policial/>. Acesso em: 30 maio 2020.

[11] BUFFON, Jaqueline Ana. Agente infiltrado virtual. *Crimes cibernéticos*, Brasília, v. 3, 2018, p. 74-91.

[12] BUFFON, Jaqueline Ana. Agente infiltrado virtual. *Crimes cibernéticos*, Brasília, v. 3, 2018, p. 74-91.

Nem todas os dados que estão no mundo virtual são verdadeiros. Assim, para que as informações sejam úteis à investigação, Alessandro Gonçalves Barreto sugere a adoção de diversas medidas.

Primeiramente o policial deve filtrar o conteúdo, realizando a pesquisa com termos precisos e claros. Também deve utilizar o instrumento de busca ou aplicação de internet da forma correta. Para tanto, o autor recomenda o uso de buscadores conhecidos, para que os resultados sejam mais precisos. Além disso, o policial deve considerar as informações do aplicativo que hospeda o conteúdo a ser procurado.[13]

O autor também sugere a criação de alertas que possibilitam que a busca por determinado termo seja enviado diretamente para o e-mail da pessoa que a solicitou. Por fim, esclarece que a coleta desses dados deve ser formalizada por meio de relatório de missão policial, contendo dados sobre o conteúdo pesquisado, metodologia utilizada, data e hora da coleta, dentre outros.[14]

A utilização de fontes abertas de informação também está sendo gradualmente adotada pelos serviços de Inteligência. Como esclarece Leonardo Singer Afonso, as fontes abertas se revelam capazes de conduzir a conclusões tão estratégicas quanto as fontes sigilosas. Muitas vezes, notícias em jornais são baseadas em informações secretas que vazaram.[15]

---

[13] BARRETO, Alessandro Gonçalves. Utilização de fontes abertas na investigação policial. **Direito & TI – Debates Contemporâneos.** Disponível em: <http://direitoeti.com.br/artigos/utilizacao-de-fontes-abertas-na-investigacao-policial/>. Acesso em: 30 maio 2020.

[14] BARRETO, Alessandro Gonçalves. Utilização de fontes abertas na investigação policial. **Direito & TI – Debates Contemporâneos.** Disponível em: <http://direitoeti.com.br/artigos/utilizacao-de-fontes-abertas-na-investigacao-policial/>. Acesso em: 30 maio 2020.

[15] A título de exemplo, o autor cita o vazamento ocorrido no Washington Times, pelo jornalista Bill Gert, que transformou documentos sigilosos em fontes abertas,

Porém, a utilização de fontes abertas, apesar de importantes, nem sempre são suficientes. O cruzamento de informações entre as fontes abertas e fechadas pode ser muito importante para o esclarecimento de delitos virtuais.

Seja para validação de dados ou para sua complementação, principalmente em investigações de grande complexidade, será necessário o acesso às fontes fechadas, utilizando-se, para tanto, o agente infiltrado virtual.

3.2 Agente Infiltrado Virtual

O agente infiltrado "é um membro do corpo policial que, para desbaratar a atividade de grupos criminosos, ingressa no grupo e participa de suas atividades até a colheita de elementos probatórios suficientes para a persecução penal".[16]

No ordenamento jurídico a infiltração de agentes foi prevista inicialmente na Lei de Drogas (tanto na revogada Lei nº 9.034/95 quanto na Lei nº 11.343/2006), porém sem qualquer regulamentação.[17]

Em 2013 a Lei de Organização Criminosa (Lei nº 12.850/2013) previu a infiltração de agentes como meio de obtenção de prova e regulamentou o tema. Estabeleceu a necessidade de autorização judicial, o prazo da medida, os direitos

e uma situação ocorrida durante a Segunda Guerra Mundial, no qual um oficial do Office of Strategic Services mostrou ao almirante que o uso do bombardeio B-29, secreto para a Inteligência e as forças armadas norte-americanas, era informação pública no Japão, onde foi veiculada por uma rádio. AFONSO, Leonardo Singer. Fontes abertas e Inteligência de Estado. *Revista Brasileira de Inteligência.* Brasília: Abin, v. 2, n. 2, abr. 2006, p. 49-62.

[16] GRECO FILHO, Vicente, **Comentários à Lei de Organização Criminosa:** *Lei n. 12.850/13,* 1ª ed. São Paulo: Saraiva, 2014. p. 58.

[17] GRECO FILHO, Vicente, **Comentários à Lei de Organização Criminosa:** *Lei n. 12.850/13,* 1ª ed. São Paulo: Saraiva, 2014. p. 58.

do agente infiltrado e a responsabilização pela eventual prática de crime.

Em 2017, por meio da alteração legislativa promovida pela Lei nº 13.441/2017, passou-se a prever a possibilidade do agente infiltrado virtual no Estatuto da Criança e do Adolescente (ECA) para a investigação de crimes contra a dignidade sexual da criança e do 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).

Em 2019, o "Pacote Anticrime", como ficou conhecida a Lei nº 13.964/209, acrescentou à Lei de Organização Criminosa a figura do agente de polícia infiltrado virtual para o combate aos crimes praticados por organizações criminosas.

A infiltração de agentes é prevista como medida excepcional, pois constitui violação à privacidade, direito individual fundamental (art. 5º, X, CF). Logo, esse meio somente deverá ser aplicado caso as outras técnicas tradicionais de investigação sejam ineficazes.[18]

A infiltração deverá ser realizada por agente policial, entendendo-se como os membros das corporações elencadas no

[18] Art. 10-A, § 3º. BRASIL. **Lei 12.850, de 02 de agosto de 2013.** Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em: 02 jun. 2020.
Art. 190-A, § 3º. BRASIL. **Lei nº 8.069, de 13 de julho de 2019.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm#:~:text=LEI Nº 8.069, DE 13 DE JULHO DE 1990.&text=Dispõe sobre o Estatuto da,Adolescente e dá outras providências.&text=Art. 1º Esta Lei dispõe,à criança e ao adolescente.&text=Nos casos expressos em lei,e um anos de idade.>. Acesso em: 02 jun. 2020.

art. 144 da Constituição Federal que possuem atribuições investigativas, quais sejam, polícia federal e polícia civil.[19]

Para a utilização desse instrumento, é preciso que haja autorização judicial, devidamente fundamentada, que estabelecerá os limites de atuação do agente. O requerimento deverá ser feito pelo Delegado de Polícia, sendo necessário parecer do Ministério Público, ou pelo Ministério Público, não sendo possível ao juiz determinar, de ofício, a medida.[20]

A decisão judicial também deverá estabelecer os limites e alcance da atuação do agente policial. Além disso, a Lei de Organização Criminosa determina que sejam especificados os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.[21]

Note-se que, na prática, a indicação dos limites e alcance da atuação do agente infiltrado pode ser bem complicada. Além da imprevisibilidade inerente a ação, não seria viável que o agente tivesse que buscar autorização judicial para cada situação vivida na infiltração. [22]

Por mais que haja uma ideia inicial dos delitos e práticas que o agente infiltrado irá se deparar, os acontecimentos são

[19] ROSSATO, Luciano Alves**. Estatuto da criança e do adolescente***: Lei n. 8.069/90 – comentado artigo por artigo.* 11ª ed. São Paulo: Saraiva, 2019, p. 533.

[20] NUCCI, Guilherme de Souza. **Estatuto da Criança e do Adolescente***,* 4ª ed. rev. atual. e ampl. Rio de Janeiro: Forense, 2018, p. 714.

[21] Art. 10-A. BRASIL. **Lei 12.850, de 02 de agosto de 2013.** Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em: 02 jun. 2020.

[22] ROSSATO, Luciano Alves**. Estatuto da criança e do adolescente***: Lei n. 8.069/90 – comentado artigo por artigo.* 11ª ed. São Paulo: Saraiva, 2019, p. 534.

dinâmicos e, muitas vezes, exigem do policial atitudes precisas e oportunas para ganhar a confiança dos agentes criminosos ou para colheita de provas.

Diante disso, a fim de acompanhar a atuação do agente, tanto a Lei de Organização Criminosa quanto o Estatuto da Criança e do Adolescente permitem ao Ministério Público ou ao Juiz requisitar, a qualquer tempo, relatório da atividade de infiltração.[23]

A respeito do prazo para a diligência, pela legislação da criança e do adolescente, a infiltração não poderá exceder o prazo de 90 dias, sem prejuízo de eventuais renovações, desde que não ultrapasse 720 dias no total.[24]

A Lei de Organização Criminosa estabelece um prazo de 6 meses, sem prejuízo de eventuais renovações, tanto para o agente infiltrado no meio físico quanto no meio cibernético.[25]

---

[23] Art. 190-A, § 1º. BRASIL **Lei nº 8.069, de 13 de julho de 2019.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm#:~:text=LEI Nº 8.069, DE 13 DE JULHO DE 1990.&text=Dispõe sobre o Estatuto da,Adolescente e dá outras providências.&text=Art. 1º Esta Lei dispõe,à criança e ao adolescente.&text=Nos casos expressos em lei,e um anos de idade.>. Acesso em: 02 jun. 2020.
Art. 10-A, § 6º. BRASIL. **Lei 12.850, de 02 de agosto de 2013.** Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em: 02 jun. 2020.

[24] Art. 190-A, inciso III. BRASIL **Lei nº 8.069, de 13 de julho de 2019.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm#:~:text=LEI Nº 8.069, DE 13 DE JULHO DE 1990.&text=Dispõe sobre o Estatuto da,Adolescente e dá outras providências.&text=Art. 1º Esta Lei dispõe,à criança e ao adolescente.&text=Nos casos expressos em lei,e um anos de idade.>. Acesso em: 02 jun. 2020.

[25] Art. 10, § 3º e art. 10-A, § 4º. BRASIL. **Lei 12.850, de 02 de agosto de 2013.** Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em: 02 jun. 2020.

Porém, somente estabeleceu-se um prazo máximo total (720 dias) para o agente infiltrado virtual. Caberá, portanto, à jurisprudência definir se o prazo máximo será aplicado para infiltração do agente fora do âmbito digital, ou não.

O procedimento de infiltração será sigiloso e apenas o Juiz, Ministério Público e Delegado de Polícia poderão ter acesso aos autos. Desse modo, a defesa terá acesso às informações somente após o oferecimento de denúncia, assegurando-se a preservação da identidade do agente e a intimidade das crianças e adolescentes envolvidas, no caso de crimes contra a dignidade sexual da criança e do adolescente.[26]

A respeito das condutas praticadas pelo policial, a Lei de Organização Criminosa prevê a responsabilização do agente pelos excessos praticados, quando não guardar a devida proporcionalidade com a finalidade da investigação. O parágrafo único do artigo 13 prevê, ainda, que não será punível, no âmbito da infiltração, a prática de crime pelo agente infiltrado no curso da investigação, quando inexigível conduta diversa.

[26] Ar. 10 c/c art. 12. BRASIL. **Lei 12.850, de 02 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em: 02 jun. 2020.
Art. 190-B c/c art. 190-E. BRASIL. **Lei nº 8.069, de 13 de julho de 2019.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm#:~:text=LEI Nº 8.069, DE 13 DE JULHO DE 1990.&text=Dispõe sobre o Estatuto da,Adolescente e dá outras providências.&text=Art. 1º Esta Lei dispõe,à criança e ao adolescente.&text=Nos casos expressos em lei,e um anos de idade.>. Acesso em: 02 jun. 2020.

Como esclarece Vicente Greco Filho, a análise da proporcionalidade deve considerar as circunstâncias em que o agente se encontra.[27]

Não pode ser milimétrica ou destituída de uma visão do contexto de tomada de decisão do agente, que pode colocar em risco sua vida se não agir na conformidade com os padrões da organização. A situação deve ser interpretada sempre de um ponto de vista favorável ao agente que se arrisca além do usual em seu dever funcional, sob pena de se inviabilizar a aceitação de quem quer que seja para o exercício dessa função. Aliás, o termo "proporcionalidade" está mal empregado. Deve ser entendido como "desnecessidade". Serão punidos os excessos, considerando-se como tais os atos desnecessários à finalidade da investigação. A proporcionalidade exige uma comparação, que é impossível no caso, porque a finalidade da investigação não é parâmetro para o tipo de atos a serem praticados. O que se pode examinar é se o ato era necessário, ou não, para o sucesso da investigação e se era exigível conduta diversa como refere o parágrafo. Se era necessário e inexigível conduta diversa, não há excesso a considerar.

O Estatuto da Criança e do Adolescente, no caput do art. 190-C, estabelece que não cometerá crime o policial que oculta a sua identidade para, por meio da internet, colher indícios e materialidade dos crimes contra a dignidade sexual da criança e do adolescente.

Entretanto, o aludido artigo diz menos do que deveria. É necessária uma interpretação conjunta com o parágrafo único do

[27] GRECO FILHO, Vicente. **Comentários à Lei de Organização Criminosa:** *Lei n. 12.850/13*, 1ª ed. São Paulo: Saraiva, 2014. p. 62.

artigo 190-C e com as recentes alterações promovidas na Lei nº 12.850/2013.

Segundo o parágrafo único do artigo 190-C do ECA, o agente que deixar de observar a estrita finalidade da investigação responderá pelos excessos praticados. Sobre o tema, Luciano Alves Rossato esclarece:[28]

Aliás, se o propósito do legislador foi o de garantir a isenção de responsabilidade penal, o dispositivo é claramente incompleto, pois, durante a infiltração, é possível que o agente receba, armazene e transmita imagens pornográficas envolvendo crianças e adolescentes. É também possível que o contato do infiltrado com criminosos igualmente o leve a se comunicar com menores numa situação em que poderia se caracterizar o aliciamento ou o assédio. Nesses casos, mantidos os limites necessários para a investigação, o policial também não pode ser responsabilizado.

Considerando o disposto no parágrafo único, o autor pondera:[29]

Dessa forma, com a finalidade de identificar determinado criminoso e de comprovar que se trata de alguém que armazena e transmite imagens pornográficas de crianças e adolescentes para posteriormente submetê-los a prostituição ou outra forma de exploração sexual, o agente infiltrado pode receber tais imagens, pode armazená-las para posteriormente juntá-las ao relatório da investigação, como também pode transmiti-las caso seja necessário para não dispersar a confiança dos criminosos

[28] ROSSATO, Luciano Alves**. Estatuto da criança e do adolescente***: Lei n. 8.069/90 – comentado artigo por artigo.* 11ª ed. São Paulo: Saraiva, 2019, p. 538.

[29] ROSSATO, Luciano Alves**. Estatuto da criança e do adolescente***: Lei n. 8.069/90 – comentado artigo por artigo.* 11ª ed. São Paulo: Saraiva, 2019, p. 538.

investigados. O mesmo pode ser dito de produções pornográficas envolvendo crianças e adolescentes: se o agente policial registra, com finalidade probatória, algo que está sendo transmitido via internet não há crime de sua parte.

Se, no entanto, o agente infiltrado, além de lidar com essas imagens, decidir encontrar uma criança ou um adolescente com a finalidade de praticar atos libidinosos, ainda que sob o pretexto da investigação, parece óbvia a caracterização do excesso punível.

Diante disso, a conduta do agente, bem como os crimes e excessos praticados, deverão ser considerados diante do caso concreto. Não é razoável que o agente infiltrado responda por todos os delitos praticados, pois em sua maioria ele o faz para adquirir a confiança dos demais agentes criminosos, porém, como policial, deve evitar a prática de atos criminosos desnecessários à investigação, evitando-se, assim, os excessos.

4 QUESTÕES PRÁTICAS

4.1 Agente provocador e o flagrante preparado

Eduardo Araújo da Silva apresenta alguns elementos para o reconhecimento do flagrante provocado: a) incitação por parte do agente provocador para determinar a vontade delituosa do indivíduo provocado (elemento objetivo); b) a vontade de o agente provocador determinar a prática de um crime para possibilitar a punição do seu autor (elemento subjetivo); e, (c) a adoção de medidas de precaução para se evitar que o crime provocado se consume.[30]

[30] SILVA, Eduardo Araújo da. **Organizações Criminosas:** *Aspectos Penais e Processuais da Lei nº 12.850/2013.* 2ª ed. São Paulo: Atlas, 2015, p. 100.

Em outras palavras, trata-se de um flagrante no qual a prática criminosa foi induzida por terceiro (agente provocador) e no qual adota-se medidas para que o crime não se consuma. Segundo a jurisprudência, essa situação configuraria crime impossível.

Tal modalidade de flagrante não é aceito pelo ordenamento jurídico pátrio. Conforme entendimento esposado na Súmula 145 do Supremo Tribunal Federal, não há crime quando a preparação do flagrante torna impossível a sua consumação.[31]

Desse modo, durante a infiltração, o agente policial deve ter em mente a finalidade precípua de coleta provas e informações, evitando envolver-se na prática de atos criminosos, e tomando as cautelas necessárias para que não se transforme em agente provocador, pois tal situação poderia tornar inócuo todo o trabalho investigativo realizado.

A título exemplificativo, é interessante trazer à baila o julgamento realizado pelo Superior Tribunal de Justiça no AgRg nos EDcl nos EDcl no AGRAVO EM RECURSO ESPECIAL Nº 1.039.417/RS, de relatoria do Ministro Rogério Schietti Cruz.[32]

---

[31] SUPREMO TRIBUNAL FEDERAL. **Súmula 145.** Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/menuSumarioSumulas.asp?sumula=2119>. Acesso em: 03 jun. 2020.

[32] BRASIL. Superior Tribunal de Justiça (6. Turma). Agravo Regimental nos Embargos de Declaração nos Embargos de Declaração no Agravo em Recurso Especial. **AgRg nos EDcl nos EDcl no AGRAVO EM RECURSO ESPECIAL Nº 1.039.417/RS.** AGRAVO REGIMENTAL NOS EMBARGOS DE DECLARAÇÃO NOS EMBARGOS DE DECLARAÇÃO NO AGRAVO EM RECURSO ESPECIAL. ARTS. 241-A E 241-B, AMBOS DA LEI N. 8.069/1990. COMPETÊNCIA DA JUSTIÇA FEDERAL. TESES DE CERCEAMENTO DE DEFESA, DE QUEBRA DE CADEIA DE CUSTÓDIA E DE FLAGRANTE FORJADO. SÚMULA N. 7 DO STJ. INÉPCIA DA INICIAL. ALEGAÇÃO PREJUDICADA. FALTA DE COMPROVAÇÃO DO DISSÍDIO JURISPRUDENCIAL. DOSIMETRIA DA PENA. AUSÊNCIA DE ILEGALIDADE. AGRAVO REGIMENTAL NÃO PROVIDO. 1. A teor do entendimento majoritário desta Corte, não se admite como paradigma, para fins de comprovação do dissídio jurisprudencial, acórdão proferido em habeas corpus, uma vez que o remédio constitucional não guarda o mesmo objeto e a mesma extensão material almejados no recurso especial. 2. Inviável a apreciação, em reclamo constitucional, das teses de cerceamento de

No caso fático restou desconfigurada o flagrante preparado pois, em resumo, a) não há flagrante provocado quando o agente

defesa, de quebra de cadeia de custódia e de flagrante preparado se, antes de adentrar na discussão jurídica, sobre a interpretação de dispositivos federais pretensamente violados, é necessário reexaminar provas, afastar as premissas fáticas do acórdão recorrido e realizar inédita reconstrução dos acontecimentos, inteiramente diversa daquela narrada pelo Juiz e pelo Tribunal a quo. Incidência da Súmula n. 7 do STJ. 3. A jurisprudência desta Corte pacificou-se no sentido de que deve ser reconhecida a internacionalidade do delito do art. 241-A do ECA se a publicação do material pornográfico infanto-juvenil ocorreu em ambiente virtual conectado à internet, de amplo e fácil acesso no estrangeiro, ainda que não haja evidências de que essa conexão tenha realmente ocorrido. 4. A superveniência da sentença penal condenatória torna esvaída a pretensão de reconhecimento de inépcia da denúncia. 5. A ausência de perícia em algumas mídias apreendidas não denota nenhum cerceamento de defesa se o material não foi utilizado contra o réu nem lastreou a sentença condenatória. A falta de devassa em alguns discos evitou a maior exposição da intimidade do acusado, uma vez que seu conteúdo não foi pertinente à resolução da lide. 6. O elemento subjetivo do tipo penal foi reconhecido pelas instâncias ordinárias de forma motivada, ante a livre apreciação do conjunto probatório. Para afastar a conclusão do aresto impugnado e acolher a tese de ausência de dolo seria necessário reexaminar provas, o que encontra óbice na Súmula n. 7 do STJ. 7. Deferida, por autoridade judicial, a busca e apreensão de computadores, discos rígidos, mídias e quaisquer outros materiais relacionados aos fatos investigados, não se verifica ilegalidade na simples varredura realizada no computador do réu por policiais, ainda no local, para o cumprimento da diligência, na presença de testemunhas e mediante registro fotográfico. Não era obrigatória a presença do suspeito no local nem a filmagem dos agentes durante a execução do mandado. 8. Afasta-se a tese de violação do art. 59 do CP se o aumento da pena-base está calcado na análise desfavorável da culpabilidade do sentenciado e das circunstâncias do crime. Houve registro de maior censurabilidade do agente, porque ele utilizou aplicativo fechado, protegido por senha, dependente de convite para ser acessado, a denotar sua sofisticada preparação para a prática dos crimes dos arts. 241-A e 241-B, ambos do ECA. O Tribunal destacou a complexidade da transmissão do material proibido, por meio de criptografia, dado não inerente ao tipo penal, dado que denota técnica acidental mais grave da conduta, a qual pode ser difundida de várias formas (fotografia, desenho, disco compacto etc.), não necessariamente por meio quase impenetrável, que exigiu a infiltração policial para ser descoberta. 9. Não se conhece, em recurso especial, por falta de prequestionamento, as teses de mutatio libelli ou de violação do princípio da correlação se as matérias não foram analisadas no acórdão recorrido. 10. Constata-se a correta aplicação do art. 71 do CP, pois, na terceira fase da aplicação da pena, o Juiz reconheceu que a mesma conduta foi reiterada em idênticas condições de local, tempo e maneira de execução, inúmeras vezes, por mais de quatro meses. Mantém-se a fração de 2/3, tendo em vista o considerável montante das ações delitivas (centenas de imagens foram divididas com outros usuários, por meses), a denotar a prática de muito mais de sete infrações. 11. A instância ordinária explicou o critério da fixação da multa, aplicada de forma proporcional à reprimenda privativa de liberdade, em conformidade com o entendimento deste Superior Tribunal. A razão unitária da sanção foi fixada em atenção à situação econômica do acusado. Para rever a individualização da pena seria necessário cotejar provas, o que não se admite na via eleita. 12. Agravo regimental não provido. Brasília, 08 de outubro de 2019. Disponível em: <https://scon.stj.jus.br/SCON/jurisprudencia/doc.jsp>. Acesso em: 02 jun. 2020.

infiltrado, devidamente autorizado, utiliza a identificação de um usuário da internet para ter acesso às comunidades virtuais fechadas e, nesse contexto, colhe provas de delitos relacionados a material de pedofilia, b) infiltração de agente para identificação dos IP's dos usuários foi judicialmente autorizada; c) o policial se limitou à identificação dos demais usuários do grupo sem necessidade de troca de e-mails ou conversas, não tendo os agentes solicitado, de forma implícita ou explicita, imagens de pornografia infantil, evitando-se incitação ao cometimento do crime; d) não restou demonstrado que a polícia interferiu no curso natural do delito; e, e) a infiltração se restringiu à fatos anteriores à medida.

Porém, muitas vezes, o limite entre o agente infiltrado e o agente provocador pode ser bem difícil de se estabelecer, principalmente quando não há elementos objetivos que demonstrem que a execução criminal por parte do investigado já havida sido iniciada.

5 CONCLUSÃO

A infiltração de agentes no meio virtual pode ser muito eficaz, principalmente nos crimes contra dignidade sexual de crianças e adolescentes e naqueles relacionados a organizações criminosas. No entanto, ela deve ser medida de *ultima ratio*.

Assim, outros mecanismos devem ser adotados inicialmente, como buscas em fontes abertas, além dos meios tradicionais de obtenção de prova, que também podem ser muito eficazes.

Porém, especialmente em delitos praticados nas fontes fechadas, como na *deep web* e na *dark web*, a investigação por

meios tradicionais pode ser incapaz de angariar os elementos probatórios necessários para a investigação.

Vale destacar que para que a medida seja deferida deve haver uma investigação prévia, devendo o Ministério Público e o Delegado de polícia apresentar elementos que comprovem a sua imprescindibilidade.

Ademais, o agente infiltrado se expõe a um risco maior do que aquele inerente as suas funções policiais e por isso tem sua identidade, imagem e qualificação protegidos, tendo direito à mudança de identidade e, no que couber, usufruir as medidas de proteção a testemunhas e até, sem necessidade de autorização do juiz, Ministério Público ou Delegado de polícia, recusar ou fazer cessar a atuação infiltrada.[33]

Por fim, para que a infiltração atinja a finalidade pretendida, o agente deve ter especial cuidado para não se tornar um agente provocador, especialmente nos casos em que a infiltração dura vários meses. O policial deverá estar qualificado e preparado para essa função, tomando todos os cuidados para que a investigação não se torne nula em razão da configuração de delito preparado.

REFERÊNCIAS

AFONSO, Leonardo Singer. Fontes abertas e Inteligência de Estado. *Revista Brasileira de Inteligência.* Brasília: Abin, v. 2, n. 2, abr. 2006, p. 49-62

BARRETO, Alessandro Gonçalves. Utilização de fontes abertas na investigação policial. **Direito & TI – Debates Contemporâneos.**

[33] Art. 14. BRASIL. **Lei 12.850, de 02 de agosto de 2013.** Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em: 03 jun. 2020.

Disponível em: <http://direitoeti.com.br/artigos/utilizacao-de-fontes-abertas-na-investigacao-policial/>.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de** Investigação **Cibernética à luz do Marco Civil da Internet**. São Paulo: Brasport, 2016.

BARRETO, Alessandro Gonçalves; WENDT, Emerson**. Inteligência Digital:** *uma análise das fontes abertas na produção de conhecimento e de provas em investigações e processos*. Rio de Janeiro: Brasport, 2017.

BITENCOURT, Cezar Roberto. **Comentários à Lei de Organização Criminosa***: Lei 12.850/2013*. São Paulo: Saraiva, 2014.

BRASIL. **Lei 12.850, de 02 de agosto de 2013.** Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>.

BRASIL**. Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>.

BRASIL. **Lei nº 8.069, de 13 de julho de 2019.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>.

BRASIL. Superior Tribunal de Justiça (6. Turma). **AgRg nos EDcl nos EDcl no AGRAVO** EM **RECURSO ESPECIAL Nº 1.039.417/RS.** Brasília, 08 de outubro de 2019. Disponível em: <https://scon.stj.jus.br/SCON/jurisprudencia/doc.jsp>.

BUFFON, Jaqueline Ana. Agente infiltrado virtual. **Crimes cibernéticos**, Brasília, v. 3, 2018, p. 74-91.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011.

GRECO FILHO, Vicente, **Comentários à Lei de Organização Criminosa:** *Lei n. 12.850/13,* 1ª ed. São Paulo: Saraiva, 2014.

KUNRATH, Josefa Cristina Tomaz Martins**. A expansão da criminalidade no cyberespaço.** Feira de Santana: Universidade Estadual de Feira de Santana, 2017.

NUCCI, Guilherme de Souza**. Estatuto da Criança e do Adolescente***,* 4ª ed. rev. atual. e ampl. Rio de Janeiro: Forense, 2018.

ROSSATO, Luciano Alves**.** Estatuto **da criança e do adolescente***: Lei n. 8.069/90 – comentado artigo por artigo.* 11ª ed. São Paulo: Saraiva, 2019.

SILVA, Eduardo Araújo da. Organizações **Criminosas:** *Aspectos Penais e Processuais da Lei nº 12.850/2013.* 2ª ed. São Paulo: Atlas, 2015.

SUPREMO TRIBUNAL FEDERAL. **Súmula 145.** Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/menuSumarioSumulas.asp?sumula=2119>. .

DEEP WEB E O MUNDO DO CRIME

Cléofanny Souza Silva[1]

RESUMO

O presente artigo busca analisar pontos desconhecidos por aqueles que não utilizam a modalidade da rede deep web, explicando um pouco sobre a "internet do submundo" nome dado por aqueles que utilizam essa modalidade de rede. Será abordado a evolução da internet em busca de entender um pouco sobre sua sistemática e construção, e alguns mecanismos para ter acesso a essa rede, desmistificando certos assuntos e demonstrando problemas significativos dentro desse mundo. A partir disso, o objetivo desse trabalho é verificar os principais delitos cometidos nesse submundo, bem como a atuação da polícia para combater esses crimes, expondo as dificuldades que os agentes encontram durante as investigações, principalmente na questão de identificar os autores, bem como uma análise sobre as técnicas de investigação para encontrar os criminosos que utilizam dessa rede para cometer diversos delitos utilizando mecanismos de proteção para burlar a lei e eventuais sanções penais. Será abordado também a legislação utilizada para punir e investigar os crimes cibernéticos.

Palavras-chave: Deep web. Crimes. Investigação.

[1] Bacharel em Direito pelo Centro Universitário de Brasília – UniCEUB. Aluna da pós graduação *lato sensu* em Direito Penal e Controle Social pelo UniCEUB. Aluna da pós graduação *lato sensu* em Direito Processual Civil pelo Centro Universitário UDF. E-mail: gabriellafbatista@gmail.com.

ABSTRACT

This article seeks to analyze points unknown to those who do not use the deep web network modality, explaining a little about the "internet of the underworld" name given by those who use this network modality. The evolution of the internet will be approached in an attempt to understand a little about its systematics and construction, and some mechanisms to access this network, demystifying certain issues and demonstrating significant problems within this world. Based on that, the objective of this work is to verify the main crimes committed in this underworld, as well as the police's action to combat these crimes, exposing the difficulties that the agents encounter during the investigations, mainly in the matter of identifying the authors, as well a analysis of investigation techniques to find criminals who use this network to commit various crimes using protection mechanisms to circumvent the law and possible criminal sanctions. The legislation used to punish and investigate cybercrimes will also be addressed.

Keywords: Deep web. Crimes. Investigation.

1 INTRODUÇÃO

Estamos vivendo na era dos avanços tecnológicos e com isso vem a importância da internet no nosso cotidiano, apesar dos diversos benefícios que essa era vem nos trazendo é necessário certo cuidado para não se tornar uma vítima desse novo mundo.

É inegável os diversos benefícios que a internet pode trazer, mas também é a traves dela que diversos crimes ocorrem diariamente em velocidade absurda. Na deep web não é diferente, muito pelo contrário, é lá que delitos graves se concretizam e por se tratar de uma internet de certa forma diferenciada conhecida por alguns como "terra de ninguém" que se encontra grandes dificuldades de pegar os autores desses crimes.

2 HISTÓRIA DA DEEP WEB

Os primeiros relatos sobre o surgimento da internet vêm do ano de 1969, onde a primeira rede foi criada. Com o passar dos

anos foi evoluindo e em 1989, após 20 anos de tal criação surgiu a ideia de transformar internet em algo mais acessível com apenas um clique e foi nesse momento que surgiu o conhecido www, desde então começou a existir debates cerca dos mistérios da internet e sua funcionalidade em especifico sobre a deep web [2]

A deep web é uma rede diferenciada, pois o conteúdo contido dentro dela é invisível pelos meios de pesquisa convencional (Yahoo, Google, etc.), isso porque é necessário mecanismo próprio para acessar essa parte da internet por se tratar de uma área mais profunda, ela é baseada na descentralização (pois dispensa a necessidade de um servidor central), anonimato, segurança (conexão criptografada ponto a ponto) e código aberto (poder de mutação e aperfeiçoamento das outras características), vejamos:

> A deep web, portanto, composta por redes de computadores que têm como características o anonimato, a criptografia, a descentralização e o codificação aberta, e cujo conteúdo não é "visível" pelas ferramentas de buscas convencionais. A arquitetura de redes predominantes é o ponto a ponto (P2P), ou seja, dispensa um servidor central, cenário no qual todos os componentes (pontos ou nós) funcionam ara como cliente, ora como servidor[3].

Dentro da deep web podemos encontrar a dark web, é essa parte da rede que importa para esse presente trabalho, uma vez que, dentro dela é exigido um elevado grau de anonimato e segurança, o que é utilizado para o cometimento de crimes, existem redes, por exemplo na dark net que é tão segurança que somente tem acesso um público selecionado.

> A rede Freenet, por exemplo, possui essa função. Nesse modo de funcionamento, os usuários

[2] BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. *Deep Web: Investigação no submundo da internet.* Rio de Janeiro: ED. BRASPORT, 2019, pg 15.

[3] Ibidem, p.17

> devem ser considerados "amigos de confiança" para. Só assim, poderem fazer parte dela. Os demais usuários sequer saberão da existência desta dark net, tampouco qual o tipo de conteúdo compartilhado. Dessa forma, o conceito de dark net abrange não só o conteúdo altamente sensível (imoral, ilegal, secreto ou restrito a apenas um grupo de usuários), mas também o alto grau de anonimato e segurança exigidos pelos componentes dessa rede "obscura".[4]

Existem varias redes que são postar para acessar a deep web, as mais conhecidas são o Tor, Freenet (citada logo acima) e o I2P.

A rede de comunicação Tor é semelhante aos navegadores padrões, como a nossa velha conhecida plataforma internet explorer, ele tem como característica apagar os rastros que a conexão entre cliente e servidor geram ao se comunicarem, sendo assim, o anonimato e segurança estão presentes em tal rede, além disse é interessante destacar que é possível usar dessa rede para navegar na internet comum de forma anônima o que impede a coleta de dados evitando eventuais importunos[5], sejamos:

> Portanto, observou-se que a principal função da rede Tor é, através da construção de um circuito de nós, utilizando comunicação criptografada, garantir a segurança e o anonimato dos pacotes de dados dos usuários, posto que o IP capturado pelas aplicações na internet será qualquer outa distinto daquela que fez a requisição[6].

A mecânica de funcionamento da rede de comunicação Freenet se difere da anterior mencionada, pois não possui um navegador próprio, o softwere dessa rede funciona conjuntamente com um navegador já existente, ou seja, é utilizada de forma conjunta com a plataforma de navegação já existente na maquina

[4] Ibidem, p.18.
[5] Ibidem, p.28.
[6] Ibidem, p.30.

do usuário (Google Chromer, Mozilla Firefox, etc.), isso porque a rede foi criada especificamente para navegar na deep web[7].

Como nas demais redes que são usadas para entrar nesse universo "desconhecido" da internet o Freenet visa também a segurança e o anonimato, ela permite que seja criado grupos fechados, ou seja, somente é permitido determinados usuários que são selecionados rigorosamente para acessarem os conteúdos compartilhados em determinados sites.

O interessante dessa rede é o conceito de liberdade que ele prega:

> Os conceitos da Freenet se apoiam na ideia de que, em alguns países, devido ao crivo do governo, muitas pessoas são cerceadas de expressarem livremente os seus pensamentos, seja por questões culturais, religiosas ou até mesmo políticas, sofrem uma censura prévia ou uma perseguição posterior, em razão do conteúdo que publicam ou acessam na ïnternet comum"[8].

Apesar dos estereótipos que esse tipo de rede carrega, como, por exemplo, ser utilizado somente para fins ilícitos é interessante ter essa visão mais humana e social que tal rede tem como pilar, ela busca uma comunicação aberta entre os usuários onde ali se torna um ambiente seguro para compartilhamento de informações e de pensamentos, afinal, não é em todo lugar que a liberdade de expressão é aceita[9].

Geralmente tendemos a enxergamos as coisas de dentro da nossa "bolha social" e esquecemos que fora dela existem lugares onde o mínimo de liberdade não é respeitada ou aceita, existe um anseio por aqueles censurados para poderem se expressar e

7 Ibidem, p.39-41.
8 Ibidem, p.39.
9 Ibidem, p.43-52.

buscar conhecimento em certos locais geográficos. Vivemos na era do conhecimento, onde com apenas um clique você tem o mundo em suas mãos, infelizmente isso não é para todos e muito sofrem ou até mesmo morrem por tentar conquistar essa tão sonhada liberdade, seja em busca de conhecimento ou de se expressar sem sofrer represálias.

Outra forma de acessar a deep web é fazendo a instalação da a I2P (projeto internet invisível), é parecida com a Freenet pois não possui navegador próprio e é necessário a instalação do softwere, porem tem o diferencial que é a existência de varias versões, dessa forma, se adequa a qualquer maquina e atende as necessidades de qualquer usuário[10].

O interessante dessa rede é que o sistema de segurança dela possui quatro camadas de criptografia, sobre o anonimato não se diferencia das demais redes já citadas, porém, o grau de anonimato vai depender do próprio usuário e da forma que ele pretende utilizar a rede, podendo configurar para atender suas necessidades.

Vejamos:

> Como o software da rede I2P instalada, o usuário poderá criar e utilizar uma conta de e-mail que é privativa dessa rede. Além do mais, poderá navegar e publicar websites anônimos com a extensão i2p na deep web. Por fim, essa rede oferece a possibilidade de utilização de clientes IRC e integração com as de compartilhamento de arquivos P2P e Donkey, Gnutella e BitTorrent, através de um cliente (programa) integrado, além de outras funções[11].

Como podemos perceber tal rede tem várias ferramentas o que permite os usuários utilizam-la de formal normal, para as

[10] Ibidem, p.57.
[11] Ibidem, p.57.

tarefas do dia a dia ou para questões mais complexas dentro da deep web.

Essas são algumas das formas de entrar na deep web e consequentemente na dark net, claro que existem diversas redes para entrar nessa modalidade de internet e com os avanços da tecnologia a tendência é o surgimento em massa de novos meios de acesso, cada uma com sua finalidade pré-estabelecida e com um público específico.

2.1 Dificuldade em chegar aos infratores de crimes feitos através da dark net

O avanço da tecnologia sem dúvidas é de estrema importância para a sociedade, a inclusão digital vem com força total nos tempos de hoje e só tendem a crescer, sempre em busca de abrir novos caminhos para o conhecimento e solucionar problemas que um dia imaginamos ser impossível de resolver.

Não se pode negar que tal avanço digital está nos levando a uma nova era de conhecimento, um novo patamar, porém, apesar de tudo parecer fantástico e muito bom como de fato é não podemos esquecer que todo esse avanço gera algumas dificuldades e problemas que tendem a surgir sempre que algo nosso é implementado na sociedade.

Com a internet não é diferente, ela é utilizada para o bem quanto para o mal, acaba por se tornando escudo para aqueles que desejam infringir a lei e se esconder por de trás de uma tela de computador sem ser identificado e saindo impune dos atos ilegais cometidos.

Por esse motivo é importante destacar os crimes mais comuns cometidos dentro da deep web, um deles é a violação de

direitos autorais, esse tipo de crime ocorre com frequência já faz algum tempo na nossa sociedade, ele ocorre com frequência até mesmo na internet comum, afinal, quantos de nós já não baixamos arquivos que continham musicas, livros, filmes, ect?

Claro que hoje em dia com o advento da legislação esta cada vez mais difícil de obter certos arquivos na internet comum, por esse motivo a deep web é o lugar perfeito para baixar certos conteúdos, pois como já mencionado o anonimato e segurança dessa internet permitem o compartilhamento ou até mesmo comercio de arquivos sem grandes empecilhos[12].

Outro crime bastante comum é a venda de armas e afins, muitos vendedores de armas que tem lojas físicas e anda na legalidade dessa atividade comércial utilizam a deep web para a venda ilegal desses produtos, uma vez que, dentro ali existe um comércio vasto desse tipo de apetrechos e o que não falta são clientes. Os comerciantes não seguem as normas impostas pela legislação o que acaba por burlar a burocracia e fiscalização para ter uma arma, o que faz a vendar ser mais rentável pela grande quantidade vendida que é maior que as vendas das lojas físicas, sem falar que o valor de um armamento cai de forma significativa nesse mercado, tornando o comercio bem atrativo principalmente para os brasileiros que para conseguir uma arma dentro da legalidade precisa preencher vários requisitos e ter dinheiro para tanto[13].

O tráfico de drogas também está presente dentro na deep web e chega a ser um dos produtos mais vendidos, pois, se ele já esta presente escancaradamente no nosso dia a dia imagina dentro de um lugar que o comércio pode ser feito de maneira fácil e

[12] Ibidem, p.76.
[13] Ibidem, p.83.

rápida, existem sites exclusivos para venda de drogas, uma vez que, o comércio é feito de uma forma mais segura justamente pelo fato de vendedor e comprador serem protegidos pelo o anonimato, a segurança acaba sendo tanta que e muitas vezes o pagamento é feito através de Bitcoins o que dificulta mais ainda eventuais ações policiais[14].

A moeda Biticoin é utilizada comumente utilizada para fins ilícitos por causa das suas características peculiares:

> O bitcoin trata-se de uma moeda digital descentralizada, ou seja, ela não depende de um emissor central e pode ser transacionada para qualquer pessoa em qualquer parte do planeta sem intermediários, e, inclusive, sem limite de valor. Sem muito aprofundamento, para utilizá-la cada usuário terá de criar uma "carteira" (um programa). Ela serve para acumular os seus endereços bitcoin. Assim, ao criar uma carteira, o usuário receberá duas chaves: uma chave criptografada pública e outra privada. A chave pública é aquela em que o usuário informará aos outros e utilizará para efetuar suas transações e a chave privada é como se fosse a "senha" da chave pública. Como as chaves públicas são muito extensas, utiliza-se muito nessas transações o chamado "QR Code"10, que é a representação da chave pública em forma de imagem[15].

Geralmente as drogas mais vendidas em sites dentro da deep web são as drogas sintéticas (Ecstasy, MD, entre outras) até mesmo pelas características dessas drogas. O que choca ao analisar esse tipo de comércio é a forma que esses produtos são entregues aos clientes, por se tratar de um produto pequeno e de fácil manejo as entregas ocorrem muitas vezes pelos meios de entrega convencional, ou seja, pelos correios o que dificulta a ação

[14] Ibidem, p.83.

[15] Ministério Público Federal: Crimes Cibernéticos - Coletânea de artigos. Vol 3. Brasília: MPF, 2018, pg 99. Disponível em: <file:///Users/apple/Downloads/Coletanea_de_artigos_sobre_crimes_ciberneticos.pdf> Acesso em 20 de maio de 2020.

policial, afinal, já existe a dificuldade em chegar aos infratores e ainda por cima as entregas ocorrem por empresas como os correios, uma empresa com grande fluxo de encomendas que se não tiver o número de rastreio não tem como se quer interceptar o produto, além do mais, não tem como a policia interceptar todas as encomendas para saber se ali naquela correspondência tem drogas ou não[16].

Cabe lembrar que é direito de todos ter a sua privacidade[17], bem como não ter violado suas correspondências[18], direitos previstos na Carta Magna, sendo assim, dependendo do tipo de interceptação de forma indiscriminada poderá consequentemente ter uma violação a tal.

Por fim, e não menos importante é necessário falar de um crime bem delicado que ocorre com frequência na deep web, se trata de abuso e exploração sexual infantojuvenil, matérias como vídeos e fotos que contem criança e situação sexual é muito difícil de se achar na internet comum, afinal não passa despercebido pelas autoridades competentes por se tratar de um conteúdo muito

[16] Ibidem, p.78-82

[17] "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: 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"; Brasil. Constituição (1988) Constituição da República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm > Acesso em 26 de maio de 2020.

[18] "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: XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)". Brasil. Constituição (1988) Constituição da República Federativa do Brasil Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm > Acesso em 26 de maio de 2020.

repulsivo e se por acaso aparecer na internet comum é rapidamente tirada do ar, por esse motivo o comércio desse tipo de material ocorre dentro da dark net[19].

Esse material exposto em alguns sites dentro na deep web gera uma certa dificuldade em ser retirado do ar, na verdade, chega a ser impossível, uma vez que, como já dito a principal característica da deep web é a descentralização e isso dificulta a ação da policia na retirada desse tipo de conteúdo, mesmo se tal matérial for excluído ele pode ser replicado por diversas vezes. Na deep web não tem a possibilidade de se pedir ao responsável do site apague aquele conteúdo como ocorrer em alguns sites de pornografias contidos na internet comum[20].

A questão é tão seria que que existe uma força tarefa para analisar esse tipo de conteúdo exposto na internet, vejamos:

> Para entalecer parâmetros adequados, aceitos em qualquer parte do mundo, a Interpol criou critérios de classificação dos arquivos que circulam na internet envolvendo crianças e adolescentes. Assim, os países membros da Interpol, que somam cerca de cinquenta, através do grupo de agentes que atuam nesse ramo, denominado de Crimes against children, ou seja, "crimes contra crianças", classificaram como delituosos os arquivos (vídeos e fotos) de acordo com três caraterísticas: Visualmente, deve ser possível a identificação de criança em fotos ou vídeos. O foco da fotografia ou filmagem é direcionado para a genital da criança. Nas imagens há crianças em ato explícito de sexo com outra criança ou com adulto[21].

Tal ação conta com agentes do mundo todo, é uma forma de varredura na internet em busca de crianças que estão sofrendo

[19] BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. *Deep Web: Investigação no submundo da internet.* Rio de Janeiro: ED. BRASPORT, 2019, pg 83.
[20] Ibidem, p.83.
[21] Ibidem, p.84.

esse tipo de violência para retira-la desse contexto cruel, bem como localizar os autores desse tipo de abuso, infelizmente os autores desse tipo de delito vem se aprimorando dia após dia para continuar com a divulgação desse tipo de material que não para de surgir[22].

Por esse motivo:

> Quando se estiver diante de investigações relativas aos crimes de pornografia infantil, os cuidados terão que ser redobrados. Isso porque a análise das imagens e diálogos deverá ser constante e muito cuidadosa, já que podem surgir notícias de possíveis ou reais abusos sexuais com ou sem produção de imagens para posse ou compartilhamento. Nessas situações, apesar da continuação da ação controlada, a fim de se atingir o objetivo proposto, o ideal é a imediata retirada desse(s) alvo(s), com sua remessa ao competente Juízo do local de ocorrência dos delitos, diante do grave perigo à criança ou ao adolescente. Ainda, para não prejudicar o êxito da investigação virtual e a ação controlada consequente, conveniente é um contato direto com as autoridades competentes que receberão o material referente ao(s) investigado(s), explicando a origem e o motivo de não se aguardar o final da ação controlada para a execução do mandado de busca e apreensão em relação àqueles possíveis agressores de menores.[23]

Ocorre que, os crimes cometidos por esses infratores apesar de muitas vezes já serem tipificados na legislação vigente como os crimes citados acima os investigadores encontram dificuldades em identificar os criminosos e consequentemente puni-los pelos atos

[22] Ibidem, p. 85-86.

[23] Ministério Público Federal: Crimes Cibernéticos - Coletânea de artigos. Vol 3. Brasília: MPF, 2018, pg 104. Disponível em: <file:///Users/apple/Downloads/Coletanea_de_artigos_sobre_crimes_ciberneticos.pdf> Acesso em 20 de maio de 2020.

delitivos, quando não é esse o problema é a falta de normas para algumas ações que tendem a evoluir diariamente[24].

Além da legislação brasileira devemos levar em consideração a legislação de outros países, por se tratar de um crime cibernético ele pode ocorrer em qualquer canto do mundo e por esse motivo será necessário colaboração das autoridades de outros países, mais uma das dificuldades encontradas na hora da investigação desse tipo de crime:

> A dificuldade encontrada pelas autoridades na apuração dos crimes cibernéticos está na característica transnacional destes, havendo grande obstáculo na obtenção de provas ou indícios, tendo em vista não haver uma legislação unificada, considerando-se a soberania dos países. Diante da inexistência de poder coercitivo na esfera internacional, os países estabelecem tratados internacionais e acordos de cooperação. Nessa atuação, há necessidade de uma combinação entre os tratados, os princípios do direito internacional e a legislação que regulamenta as empresas privadas que atuam na internet[25].

Sabemos que a investigação é o passo inicial para as autoridades chegarem nos infratores, não é diferente com os crimes cibernéticos, nesses crimes os investigadores seguem rastros que algumas ações deixam pelo caminho, esse é o primeiro passo de uma investigação em crimes cibernéticos. Apesar de

[24] BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. *Deep Web: Investigação no submundo da internet.* Rio de Janeiro: ED. BRASPORT, 2019, pg 87.

[25] Ministério Público Federal: Crimes Cibernéticos - Coletânea de artigos. Vol 3. Brasília: MPF, 2018, pg 99. Disponível em: <file:///Users/apple/Downloads/Coletanea_de_artigos_sobre_crimes_ciberneticos.pdf> Acesso em 20 de maio de 2020.

seguir os rastros ao agentes não terão acesso ao conteúdo compartilhado e terá que descobrir isso de outra forma [26].

Por esse motivo, durante as execuções das atividades suspeitas os investigadores coletam os vestígios deixados para que na sorte encontre os criminosos. Nesse tipo de investigação e necessário de fazer a preservação de evidências, a preservação dessas provas é essencial para ter êxito nas investigações, uma vez que, como se trata de um ambiente volátil as provas podem se perder com grande facilidade e assim o risco de não chegar aos infratores e puni-los é muito grande[27].

Sendo assim, existe meios de preservar as evidências e coletar provas, no âmbito internacional as autoridades utilizam com frequência a mutual legal assistence treaty - tratado de assistência jurídica mútua (MLAT), sobre a MLAT é importante destacar:

> Um tratado de assistência jurídica mútua (MLAT) é um acordo entre dois ou mais países com a finalidade de coletar e trocar informações em um esforço para aplicar leis públicas ou criminais.
>
> Estados modernos desenvolveram mecanismos para solicitar e obter provas para investigações criminais e processos judiciais. Quando evidências ou outras formas de assistência legal, como declarações de testemunhas ou o serviço de documentos, são necessárias a um soberano estrangeiro, os estados podem tentar cooperar informalmente através de suas respectivas agências policiais ou, alternativamente, recorrer ao que é tipicamente chamado de solicitações. "Assistência Jurídica Mútua"[28].

[26] BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. *Deep Web: Investigação no submundo da internet.* Rio de Janeiro: ED. BRASPORT, 2019, pg 89.

[27] Ibidem, p.90.

[28] FORENSE, Ti. MLAT – Mutual Legal Assistance Treaty. 2018; Disponível em: <https://www.tiforense.com.br/mlat-mutual-legal-assistance-treaty/ > Acesso em 26 de maio de 2020.

O MLAT tem sua origem baseada na carta rogatória, está se trata de um instrumento jurídico onde determinado país se comunicam com outro para solicitar atuação jurisdicional para que assim ocorra o desenvolvimento de um processo, seja ele na esfera civil ou criminal[29].

Esses dois instrumentos são auxiliadores importantíssimos na esfera internacional, mas existes outros meios de coleta e preservação de provas para crimes menos complexos cometidos no âmbito nacional como, por exemplo download de imagens e vídeos, captura de links, vejamos:

> Para delitos praticados na surface, são utilizados meios de preservação de evidências: print screen, certidão do escrivão de polícia, ata notória, cooperação policial internacional, plataformas disponibilizadas pelas aplicações de internet, ofício de autoridade policial dentre outros.[30]

Por esse tipo de peculiaridade nas coletas de provas nos crimes cibernéticos é imprescindível a instauração do inquérito policial, não podendo este ser substituído, dessa forma, não imposta a gravidade do delito que está sendo apurado o primeiro passo sempre será a instauração do inquérito[31]

Geralmente a investigação na internet comum tende a ser mais fácil, pois na maioria das vezes os investigadores se valem das fontes abertas de dados, ou seja, são de livre acesso, dessa

---

[29] Ministério Público Federal: Temas de Cooperação Internacional – Coleção MPF Internacional. Vol 2. Brasília: MPF, 2015, pg 08. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/dados-da-atuacao/links-tematicos/colecao-mpf-internacional-1/temas_cooperacao_internacional_versao_online.pdf#page=11> Acesso em 26 de maio de 2020.

[30] BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. *Deep Web: Investigação no submundo da internet.* Rio de Janeiro: ED. BRASPORT, 2019, pg 88.

[31] Ibidem, p.77.

forma, os investigadores conseguem muitas informações que ajudam a solucionar crimes[32].

Importante destacar que grande massa de informações são colhidas dentro das redes sócias (Facebook, Twitter, Instagram, etc) que consequentemente auxiliam em grade parte da investigação, muitas vezes os crimes são solucionados através de agentes infiltrados nessas redes, além da cooperação dessas redes com a justiça[33].

Portanto, é de grande ajuda a utilização de dados abertos que não se restringe:

> Ressalta-se, por oportuno, que a utilização de dados de fontes abertas não é exclusividade da atividade policial. Os tribunais pátrios já vêm aceitando essa coleta para subsidiar suas decisões. No julgamento de um habeas corpus, o termo "consulta realizada em fontes abertas na rede mundial de computadores" foi empregada para comprovar a relação entre as empresas investigadas. Noutro caso, houve a individualização através de redes sociais.
>
> Inúmeros são os casos de aplicações dos dados de fontes abertas por parte do poder judiciário, dentre os quais destacamos: suspenção de auxílio-doença em razão de postagens no Facebook; localização de beneficiário da justiça do trabalho; e negativa de justiça gratuita[34].

Na dark net por se tratar de uma parte profunda da internet com certas peculiaridades alguns mecanismos de investigação não são eficientes no combate aos crimes cibernéticos ocorridos por lá, por esse motivo a infiltração dentro da rede se torna essencial para se chagar nos autores dos delitos[35].

[32] Ibidem, p.79.
[33] Ibidem, p.79.
[34] Ibidem, p.90.
[35] Ibidem, p.91.

A infiltração de agentes está prevista em algumas leis vigentes na legislação brasileira[36], para a aplicação delas é necessário o seguimento de certas regras, o que pode deixar as investigações morosas.

Inicialmente, será necessária autorização judicial para colocar um agente infiltrado, tal ação é fundada no sigilo para não colocar o agente em perigo e nem comprometer a operação, tal decisão judicial conterá os limites de atuação desse(s) agente(s) que se por acaso ultrapassar os limites impostos ou desviar dos objetivos da investigação será responsabilizado judicialmente por suas ações[37].

Para se infiltrar na rede é necessária a capacidade técnica e principalmente perspicaz em tais investigações por causa dos mecanismos de proteção que os infratores usam, além do mais técnicas comuns as vezes não são suficientes para investigação no submundo da internet:

> Investigar crimes praticados nomeio cibernético não tem sido tarefa fácil notadamente quanto os criminosos contam, para a pratica dos seus atos,

[36] "Art. 53. Em qualquer fase da persecução criminal relativa aos crimes previstos nesta Lei, são permitidos, além dos previstos em lei, mediante autorização judicial e ouvido o Ministério Público, os seguintes procedimentos investigatórios: I - a infiltração por agentes de polícia, em tarefas de investigação, constituída pelos órgãos especializados pertinentes. Brasil. Lei 11343, de 23 de agosto de 2006. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm>; Art. 190-A. A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240 , 241 , 241-A , 241-B , 241-C e 241-D desta Lei e nos arts. 154-A , 217-A , 218 , 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) , obedecerá às seguintes regras: (Incluído pela Lei nº 13.441, de 2017). Brasil. Lei 8069, de 13 de julho de 1990. Disponível em:<http://www.planalto.gov.br/ccivil_03/LEIS/L8069.htm#art190aV>; Art. 3º Em qualquer fase da persecução penal, serão permitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção da prova: VII - infiltração, por policiais, em atividade de investigação, na forma do art. 11. Brasil. Lei 12850, de 02 de agosto de 2013. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm> Acesso em 20 de maio de 2020.

[37] BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. *Deep Web: Investigação no submundo da internet.* Rio de Janeiro: ED. BRASPORT, 2019.

> com uma infinidade de ferramentas tecnológicas acessíveis de forma gratuita, garantindo-lhe o anonimato e os meios para esgueirar-se da persecução penal. Se os delitos praticados na surface web (nota de rodapé explicando o que é) já trazem consigo certos impedimentos para a atribuição de autoria delitiva, que dirá os efetivados na deep web[38].

Por esse motivo, uma das maiores dificuldades da polícia é identificar os autores dos delitos na deep web, essa dificuldade se da porque os mecanismos de segurança dos usuários são aperfeiçoados diariamente, afinal, a internet se inova a cada dia.

Sendo assim, existe uma forma de investigação que pode trazer êxito nas apurações de crime na deep web o NIT – NETWORK INVESTIGATIVE TECHNIQUE[39], que somente pode ser usada se estivar amparada por autorização judicial, pois será necessário a instalação de um software no aparelho do suspeito, através da instalação desse software será possível obter diversas informações (histórico de navegação, registro de conexão, ect.)

[38] BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. *Deep Web: Investigação no submundo da internet.* Rio de Janeiro: ED. BRASPORT, 2019, pg 92.

[39] "O governo federal dos EUA desenvolveu uma ferramenta eletrônica de computador conhecida como Técnica de investigação em rede ('NIT'). Essencialmente, um NIT é um dispositivo usado pela polícia para invadir um computador individual para obter acesso e obter todos os tipos de informações, incluindo arquivos de computador, fotos, e-mails e outros dados. Esse sucesso levou a numerosos processos contra aqueles que recebem e compartilham pornografia infantil. No entanto, em resposta, os réus estão começando a apresentar desafios à maneira como essa tecnologia funciona. Os tribunais estão lutando para definir a linha entre o direito de um réu a um julgamento justo, que poderá ser violado se o réu não tiver um entendimento adequado de como a tecnologia funciona e o interesse do governo em manter sigilo sobre as ferramentas de investigação que desenvolve." OWSLEY,Brian L. Network investigative source code and due process. Londres, 2017. Disponível em: < https://journals.sas.ac.uk/deeslr/article/view/2475/2434> Acesso em 24 de maio de 2020.

que serão de grade valia para quesito de autoria de materialidade[40].

Vejamos: "*Essa técnica para obtenção de evidencias eletrônicas já vem sendo aplicada pelo Federal Bureau of Investigation – FBI – há mais de 25 anos em casos relacionados a abuso e exploração infantojovenil, terrorismo, extorsão, dentre outros*[41]*"*.

Esse tipo de investigação é amparado pela lei 9.296/96 que abrange desde o método de investigação comum (interceptação telefônica) desde o método mais complexos (NIT) que nada mais é que a quebra de sigilo telemático, essa lei serve como parâmetro para fundamentação de ordens judiciais e é necessário cumprir de requisitos, vejamos:

> Só haverá sua admissão, contudo, caso seja evidenciado que:
>
> A prova não pode ser demonstrada por outros meios; há indícios razoáveis de autoria e participação em infração penal; o fato investigado constituí infração penal punida com reclusão[42].

Isso se da porque tal investigação é mais incisiva das tradicionais e chega a ferir o princípio constitucional da privacidade, sendo assim, não podemos utilizar dessa forma de investigação em massa devendo sempre ser utilizada nos casos que de fato só poderá extrair informações dessa forma e somente de maneira individualizada, devendo sempre ter autorização judicial e se enquadrar nos requisitos acima mencionados.

---

[40] BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. *Deep Web: Investigação no submundo da internet.* Rio de Janeiro: ED. BRASPORT, 2019, pg 95.
[41] Ibidem, p.97.
[42] Ibidem, p.98.

3 CONCLUSÃO

Como podemos perceber a internet é um marco importantíssimo para os avanços tecnológicos e consequentemente sociais, através dela muitas tarefas do dia a dia se tornaram simples, quem diria que com apenas um clique poderíamos fazer tanto?

O conhecimento que essa tecnologia nos traz é extraordinária, sem falar na velocidade que somos bombardeados de informações, o que tem um lado bom e também o seu lado ruim por muitas vezes não conseguir se quer distinguir se as informações prestadas são de fato verdadeiras.

Com o avanço da internet se tornou possível a conexão de pessoas distintas em diferentes partes do mundo em questão de frações de segundos, de certa forma ficamos mais perto das pessoas que amamos mesmo elas estando a quilômetros de distância, a comunicação ficou mais prática.

A internet comum hoje é acessada por milhões de pessoas, ocorre que muitas delas não tem o conhecimento sobre a deep web e se tem acabam não acessando por medo, afinal essa modalidade de internet está cercada de diversas informações negativas, isso acontece porque existem vários tabus envolta dessa vasta rede.

Inegável é que a internet se tornou uma arma fatal na mão daqueles que desejam fazer mal, e isso não é somente uma característica da deep web como também esta presente na internet convencional, afinal vários de nós já sofremos ou já vimos o cometimento de algum crime cibernético, seja ameaças, xingamentos, contas de rede social invadidas, fotos intimas espalhadas na web, golpes em compras de mercadorias, produtos

ilícitos sendo vendidos, entre outros problemas. Apesar dos transtornos que as vítimas desses delitos sofrem muitas vezes não se compara com as infrações graves cometidas dentro da dark net.

Por esse motivo, da mesma forma que a internet é uma "benção" ela pode se tronar um pesadelo e isso sem dúvidas nos gera inseguranças, afinal já é compilado ter as demandas do dia a dia solucionadas com êxito, quem dirá as causadas on-line.

Grande parte da população não tem acesso a deep web pelo fato de exigir do usuários demandas e cautelas ao ingressar na rede, apesar dos tabus que envolvem a deep web é sempre bom ressaltar que tal rede não é somente instrumento para se fazer o mal, mas é instrumento de liberdade para aqueles que se veem presos em uma realidade opressora, ali também é meio de se protestar, de criticar e de acessar informações proibidas e censuradas por certo governos, afinal o conhecimento se torna fonte de poder.

Além desse ponto de vista social, essa rede também se torna mecanismos de proteção de dados, utilizada por aqueles que buscam se esquivar de certas inconveniências, por exemplo, quando pesquisamos algo e de repente aquilo que você pesquisou começa a aparecer em vários lugares, nas suas redes sociais, anúncios chatos, entre outras coisas.

Infelizmente dentro dessa modalidade de rede crimes graves são cometidos e grande parte deles ficam sem a punição adequada pelo fato dos criminosos se valerem de mecanismos de proteção, o que dificulta a ações policiais, diariamente avanços são feitos por esses criminosos o que faz que a polícia tenha a necessidade de aprimorar também seus mecanismos de investigação, claro que nessa rede um dos melhores mecanismos de investigação se trata

da infiltração policial, pois apesar de antigo ainda traz bons resultados para chegar na autoria delitiva e dessa forma combater o crime dentro da dark net.

Diferente da internet comum que é possível apagar algum arquivo mesmo com as burocracias de praxe, na deep web isso não é possível, por causa de descentralização da rede, dessa forma, por tudo já dito que não é possível a atuação da polícia de forma mais incisiva e se deve ter ainda mais cautela nesse campo de investigação para não perder a oportunidade de chegar aos infratores. A investigação desses crimes cometidos na internet chega a uma linha tênue, de um lado os limites da legalidade da ação policial e do outro a criminalidade crescente na web no meio dessas suas vertentes está os direitos de um cidadão.

Decerto, limites devem ser respeitados e direitos preservados, porem não podemos negar que o avanço que estamos vivendo gera problemas não solucionados nesse campo, ou seja, se torna empecilho no combate a criminalidade e uma brecha para impunidade, o que gera uma insegurança jurídica.

Os mecanismos de combate aos crimes cibernéticos precisam ser inovados, meios tecnológicos podem e devem ser criados para solucionar esses problemas, mas a legislação também precisa avançar de forma condizente para que assim talvez tenhamos mais eficiência no combate ao crime.

A morosidade em lidar com esse assunto e enfrentar os problemas visíveis podem gerar futuramente grandes problemas, um deles, por exemplo é o número crescente de crimes cometidos na internet que não conseguimos controlar e muito menos solucionar e isso tende a ficar cada dia pior.

Deve ocorrer uma desburocratização nas ações de investigação para que pelo menos obtenhamos uma paridade perante a criminalidade, pois, enquanto demoramos anos para construir leis e coloca-las em pratica os crimes só aumentam e com isso sua impunidade também, faz necessário que o judiciário enfrente essa questão.

REFERÊNCIAS

BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. *Deep Web: Investigação no submundo da internet.* Rio de Janeiro: ED. BRASPORT, 2019

Brasil. Constituição (1988) Constituição da República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em 26 de maio de 2020.

Brasil. Lei 11343, de 23 de agosto de 2006. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm>. Acesso em 20 de maio de 2020.

Brasil. Lei 12850, de 02 de agosto de 2013. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>.Acesso em 20 de maio de 2020.

Brasil. Lei 8069, de 13 de julho de 1990. Disponível em:<http://www.planalto.gov.br/ccivil_03/LEIS/L8069.htm#art190aV>. Acesso em 20 de maio de 2020.

FORENSE, Ti. MLAT – Mutual Legal Assistance Treaty. 2018; Disponível em: <https://www.tiforense.com.br/mlat-mutual-legal-assistance-treaty/ >. Acesso em 26 de maio de 2020.

Ministério Público Federal: Crimes Cibernéticos - Coletânea de artigos. Vol 3. Brasília: MPF, 2018, pg 99. Disponível em: <file:///Users/apple/Downloads/Coletanea_de_artigos_sobre_crimes_ciberneticos.pdf>. Acesso em 20 de maio de 2020

Ministério Público Federal: Temas de Cooperação Internacional – Coleção MPF Internacional. Vol 2. Brasília: MPF, 2015, pg 08. Disponível em: <http://www.mpf.mp.br/atuacao-

tematica/sci/dados-da-atuacao/links-tematicos/colecao-mpf-internacional-1/temas_cooperacao_internacional_versao_online.pdf#page=11>. Acesso em 26 de maio de 2020.

OWSLEY,Brian L. *Network investigative source code and due process.* Londres, 2017. Disponível em: < https://journals.sas.ac.uk/deeslr/article/view/2475/2434>. Acesso em 24 de maio de 2020.

SANNINI NETO, Francisco. *Infiltração de agentes é atividade de polícia judiciária*. Disponível em: <https://canalcienciascriminais.com.br/infiltracao-de-agentes-e-atividade-de-policia-judiciaria/>. Acesso em 20 de maio de 2020.

A PORNOGRAFIA DE VINGANÇA COM UM OLHAR SOB A VÍTIMA

Nathália de Andrade Silva Anastácio[1]

RESUMO

O presente artigo traça um panorama geral a respeito da pornografia de vingança que constitui-se como mais uma forma de violência de gênero. Primeiro se encarrega de conceituar o crime e entender como se configura na prática. Traz a forma que o ordenamento jurídico pátrio trata essa conduta e a resposta concedida pelo Estado e pela sociedade a essas vítimas. Sempre analisando o revenge porn com um olhar sob a vítima tendo como finalidade principal a prevenção dessa prática delitiva, direcionando a conduta da vítima. Para só assim ser possível minimizar com eficiência a ocorrência dos crimes e dos consequentes danos sofridos.

Palavras-chave: Pornografia de vingança. Violência de gênero. Violência contra a mulher. Vitimologia. Prevenção.

ABSTRACT

This academic provides an overview of revenge porn which another form of gender-based violence. First, it is in charge of conceptualizing the crime and understand how it is configured in practice. It shows the way that the Brazilian legal system treats this behavior and the response granted by the state and society to these victims. Always analyzing revenge porn with a look at the victim with the main purpose of preventing this criminal practice, directing the victim's conduct. Only then will it be possible to

[1] Aluna da pós graduação em Direito do Instituto Ceub de Pesquisa e Desenvolvimento – ICPD/UniCEUB.

minimize efficiently the occurrence of crimes and damages suffered.

Keywords: Revenge porn. Gender violence. Violence against woman. Victimology. Prevention.

1 INTRODUÇÃO

A pornografia de vingança do termo em inglês "*revenge porn*", consiste no ato de divulgar conteúdo íntimo ou de nudez com o intuito de se vingança. Apesar de não ser uma conduta recente faz pouco tempo que esse crime ganhou a atenção da mídia e do ordenamento jurídico.

O presente artigo busca sobretudo analisar a pornografia de vingança com um olhar sob a vítima. Para isso busca conceituar esse crime, analisar a sua aplicação na prática, sua relação com a violência de gênero e principalmente os danos emocionais, sociais e profissionais experimentados pelas mulheres vítimas do *revenge porn*.

O objetivo principal é a trazer para o debate a possibilidade de prevenir esse crime interferindo na conduta da vítima, cuja finalidade é diminuir o número de mulheres que têm suas vidas transformadas após a divulgação desses materiais de cunho sexual, sem a sua autorização.

No primeiro tópico será abordado o crime da pornografia de vingança e a sua relação com a violência de gênero. O crime será conceituado e far-se-á um breve apanhado sobre a sua origem, uma análise de como ocorre na prática e sua ligação com a violência contra a mulher para que se possa compreender porque o crime aparece como o atual instrumento de inferiorização e humilhação da mulher frente a sociedade.

Em seguida, passa-se a análise do controle desse crime pelo ordenamento jurídico pátrio desde o momento anterior a sua tipificação até o momento atual, bem como o tratamento dispensado a vítima ao longo do processo, além de questionar a efetividade da resposta dada pelo Estado através do poder judiciário.

Mais adiante discute-se a importância da vítima para a concretização do fenômeno criminológico, a partir da perspectiva trazida pela ciência da vitimologia e a prevenção vitimária. Por fim, serão abordados possíveis caminhos para a prevenção do *revenge porn*.

1.1 Pornografia de vingança e a violência de gênero

A pornografia de vingança advém da expressão em inglês *revenge porn* e consiste no ato de divulgar e disseminar na internet conteúdo privado de uma pessoa, sem sua autorização, contendo cenas de nudez ou sexo, podendo ser fotos, vídeos, montagem dentre outros materiais sexuais, íntimos e privado de uma pessoa.[2] Sendo caracterizada como uma forma de violência moral com cunho sexual.[3]

O termo "pornografia-não-consensual" por vezes é utilizado como sinônimo do termo "pornografia de vingança". Advém que, o primeiro é gênero e abarca tanto a distribuição de vídeos ou

[2] BUZZI, Vitória de Macedo. **Pornografia de vingança**: Contexto histórico-social e abordagem no Direito Brasileiro. 2015. 110 f. Monografia (Bacharelado em Direito) - Centro de Ciências jurídicas, Universidade Federal de Santa Catarina, Florianópolis.

[3] CRESPO, Marcelo. **Revenge Porn. A Pornografia da vingança**, 2014. Disponível em: <http://marcelocrespo1.jusbrasil.com.br/artigos/153948423/revenge-porn-a-pornografia-da-vinganca> Acesso em maio.2020

imagens sexualmente gráficas, registrados originalmente sem o consentimento do indivíduo, como, por exemplo, gravações escondidas ou gravações de agressões sexuais. Quanto aqueles conteúdos registrados originalmente com o consentimento, geralmente no contexto de um relacionamento íntimo e que após é distribuído sem o consentimento do envolvido.[4]

À vista disso, a vingança pornográfica, objeto desse artigo, é uma espécie que abarca apenas a divulgação e disseminação de conteúdo sexual e nudez sem o consentimento da pessoa envolvida. Com o objetivo de expor a vítima através da rápida disseminação do conteúdo nas redes sociais, e assim causar danos sociais e emocionais na vida da vítima cujos, efeitos são irreparáveis.[5]

Importante salientar que a conduta consiste em se utilizar de um material, prévia e voluntariamente, angariado no decorrer de um relacionamento íntimo com o objetivo de vingança.[6] Portanto, o crime se configura independente de um consentimento anterior para a produção do material.

Apesar de ser um crime rápido viola os direitos à privacidade e à intimidade de uma forma devastadora. Além de gerar danos permanentes em suas vítimas, majoritariamente mulheres.[7] Os

[4] BUZZI, Vitória de Macedo. **Pornografia de vingança**: Contexto histórico-social e abordagem no Direito Brasileiro. 2015. 110 f. Monografia (Bacharelado em Direito) - Centro de Ciências jurídicas, Universidade Federal de Santa Catarina, Florianópolis.

[5] Idem.

[6] NUCCI, Amanda Ferreira de Souza; TEIXEIRA, Leonardo de Aquino. **Uma análise sobre revenge porn e a eficácia dos mecanismos jurídicos de repressão.** Revista Consultor Jurídico, 2019. Disponível em:<https://www.conjur.com.br/2019-jul-30/opiniao-revenge-porn-eficacia-mecanismos-repressao> Acesso em maio.2020.

[7] VARELLA, G; SOPRANA, P. **Pornografia de Vingança: crime rápido, trauma permanente** [online]. São Paulo, 16 Fev 2016. Fonte: Época. Disponível em:

conteúdos sexuais submetidos a rápida visualização sem o consentimento da vítima, por vezes contam com informações pessoais da vítima com o objetivo de humilhá-la publicamente e desmoralizá-la, sobretudo após o fim do relacionamento.[8]

De início, cabe ressaltar que não se tem uma data exata sobre o início da prática da pornografia de vingança. A ideia que se tem é que o crime se iniciou, por volta dos anos 2000, entre os usuários da *Usenet*, onde os próprios membros começaram a compartilhar fotos e vídeos de suas ex-namoradas. Os vídeos se destacavam por sua autenticidade e realismo total nomeado por *realcore pornography*.[9]

Em 2008 o site XTube informou o recebimento de reclamações feitas por mulheres que diziam terem sido expostas, sem sua autorização, em vídeos hospedados no referido site. Alegando ainda que haviam sido vítimas de seus ex-parceiros.[10]

A intenção da pessoa que divulga esses conteúdos, em sua maioria homens, é causar uma degradação moral da vítima frente a sociedade após o término de um relacionamento.[11] Infelizmente, a pessoa que o fez não é recriminada e sim a que sofreu o dano. A sociedade se encarrega de concretizar a exclusão da vítima, como se a culpa da divulgação fosse dela, por ter permitido a produção desses materiais.

<http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/02/pornografia-de-vinganca-crime-rapido-trauma-permanentee.html>Acesso em maio.2020.

[8] BUZZI, Vitória de Macedo. **Pornografia de vingança**: Contexto histórico-social e abordagem no Direito Brasileiro. 2015. 110 f. Monografia (Bacharelado em Direito) - Centro de Ciências jurídicas, Universidade Federal de Santa Catarina, Florianópolis.

[9] *Idem.*

[10] Idem.

[11] Idem.

A primeira sentença de prisão em razão da publicação online de conteúdo pornográfico com objetivo de vingança ocorreu apenas em 2010.[12] O neozelandês Joshua Ashby, de 20 anos, ameaçou sua namorada de morte após o fim do relacionamento de cinco meses. Posteriormente, acessou a conta da vítima no site do *Facebook*, alterou a foto de perfil por uma foto nua que a ex-companheira havia o enviado durante o relacionamento e trocou a senha da conta para que a vítima não pudesse retirar a foto. A conta foi encerrada após 12 horas pela polícia e pelo Facebook, mas a foto já havia viralizado.[13]

A atenção da mídia internacional só veio após a criação do site *IsAnyoneUp* (Tem alguém afim?) pelo australiano Hunder Moore. O site, autointitulado "especializado em pornografia de vingança" permitia que os usuários enviassem fotos de pessoas nuas, em sua maioria mulheres, que eram disponibilizadas para acesso livre de todos os visitantes. Após a certificação de que a vítima era maior de 18 anos e incluía informações pessoais das vítimas junto com as fotos.[14]

Apesar de vários precedentes, com certeza um dos mais relevantes ocorreu apenas em 2015. Kevin Bollaert, de 29 anos, foi condenado definitivamente a uma pena de 8 anos de reclusão e

[12] BUZZI, Vitória de Macedo. **Pornografia de vingança**: Contexto histórico-social e abordagem no Direito Brasileiro. 2015. 110 f. Monografia (Bacharelado em Direito) - Centro de Ciências jurídicas, Universidade Federal de Santa Catarina, Florianópolis.

[13] Disponível em: <http://www.dailymail.co.uk/news/article-1329812/Joshua-Ashby-Facebook-user-jailedposting-naked-picture-ex-girlfriend.html> Acesso em maio.2020

[14] BUZZI, Vitória de Macedo. Pornografia de vingança: Contexto histórico-social e abordagem no Direito Brasileiro. 2015. 110 f. Monografia (Bacharelado em Direito) - Centro de Ciências jurídicas, Universidade Federal de Santa Catarina, Florianópolis.

mais 10 anos de supervisão por 27 acusações, incluindo roubo de identidade e extorsão.[15]

O condenado era proprietário e administrador de dois sites de pornografia da vingança: o *ugotposted.com* onde os usuários podiam publicar fotos de nudez ou fotos íntimas das suas ex-companheiras, sem a autorização delas, para se vingar em razão do término e o *changemyreputation.com* onde ele cobrava das vítimas para retirar o conteúdo prejudicial do site anterior. Algumas fotos publicadas on-line continham inclusive informações pessoais das vítimas, a saber: nomes e as cidades onde elas moravam e trabalhavam.[16]

Logo, apesar de não ser um crime novo é perceptível que a sua punição e repercussão tanto na mídia quanto no ordenamento jurídico é muito recente, tendo sido impulsionada por sites, blogs e pelo movimento feminista.

Foi através da mídia que muitas empresas de serviços online, sites e redes de relacionamento passaram a ser expostas e confrontadas. O que levou as empresas a buscarem caminhos para coibir esse tipo de divulgação, ao editar normas mais severas relacionadas ao compartilhamento de material pornográfico não autorizado.[17]

Desde o início a pornografia da vingança, notoriamente, atinge um número muito maior de mulheres do que de homens.

---

[15] WINKLEY; Lyndsay; LITTLEFIELD, Dana. ***Sentence revised for revenge porn site operator.*** postado em 21 set. 2015. Disponível em https:<//www.sandiegouniontribune.com/sdut-kevin-bollaert-revenge-porn-case-resentencing-2015sep21-story.html>Acesso em maio.2020.

[16] *Idem.*

[17] BUZZI, Vitória de Macedo. Pornografia de vingança: Contexto histórico-social e abordagem no Direito Brasileiro. 2015. 110 f. Monografia (Bacharelado em Direito) - Centro de Ciências jurídicas, Universidade Federal de Santa Catarina, Florianópolis.

Apesar disso, apenas recentemente é que tal conduta passou a ser vista como uma forma de violência contra a mulher.[18]

Em 2014 foi realizada uma pesquisa pela organização *EndRevengePorn* que oficializou esses dados e comprovou que 90% das pessoas que alegaram terem sido vítimas da pornografia da vingança eram mulheres, 57% alegaram que o conteúdo pornográfico foi divulgado por um ex-companheiro e 59% contendo informações pessoais da vítima. Além disso 93% alegaram terem sofrido estresses e problemas emocionais, 82% ter sofrido danos na sua vida social e 57% disseram ter medo de que fossem prejudicadas profissionalmente em razão da violência sofrida.[19]

A violência de gênero é definida como qualquer ato violento em função do gênero ao qual pertencem as pessoas envolvidas seja mulher ou homem.[20] A violência contra a mulher é definida pela Convenção de Belém do Pará, no Decreto n° 1973, de 1996, como: "qualquer ato ou conduta baseada no gênero, que cause morte, dano ou sofrimento físico, sexual ou psicológico à mulher tanto na esfera pública como na esfera privada".

Em razão das mulheres figurarem, majoritariamente, como vítimas, a violência de gênero se torna quase sinônimo de violência contra a mulher[21]. Portanto, o fenômeno da pornografia de

---

[18] *Idem.*

[19] End Revenge Porn. **A campain of the cyber civil rights initiative, inc.** Disponível em: <http://www.endrevengeporn.org/main_2013/wpcontent/uploads/2014/12/RPStatistics.pdf> Acesso em maio.2020

[20] KHOURI, José Naaman. **Violência contra a mulher**. MidiaNews, 14 de fevereiro de 2012. Disponível em: <http://www.midianews.com.br/conteudo.php?sid=262&cid=81369>. Acesso em maio.2020.

[21] KHOURI, José Naaman. **Violência contra a mulher.** MidiaNews, 14 de fevereiro de 2012. Disponível em:

vingança deve ser analisado sob a perspectiva da violência de gênero caracterizando-se como mais um instrumento de humilhação social, contra as mulheres, utilizado pelos homens.[22]

1.2 O direito brasileiro e o esquecimento da vítima

A sociedade atual é marcada pela evolução da tecnologia, sobretudo no que diz respeito a velocidade o que possibilita o surgimento de novos crimes virtuais sem que o ordenamento jurídico consiga acompanhar. O ciberespaço se apresenta como um local para cometimento de crimes, muitas vezes já tipificados, encoberto pela sensação de impunidade, principalmente, por uma grande parcela da sociedade entender a internet como uma "terra sem lei" onde é permitido fazer tudo sem ser responsabilizado.[23]

A tecnologia facilita o acesso às redes sociais e ao manejo de ferramentas de rápida transmissão da informação o que exige uma resposta do direito quanto aos novos modos de violação dos bens jurídicos já tutelados pelo ordenamento pátrio. Essas facilidades trazidas, assim como o anonimato acabam tornando a tipificação comum insuficiente. Ao se utilizar a internet esses crimes ganham uma proporção gigantesca e dificultam a investigação do delito, como acontece nos crimes de pornografia de vingança. Nesse

<http://www.midianews.com.br/conteudo.php?sid=262&cid=81369>. Acesso em maid.2020.

[22] BUZZI, Vitória de Macedo. Pornografia de vingança: Contexto histórico-social e abordagem no Direito Brasileiro. 2015. 110 f. Monografia (Bacharelado em Direito) - Centro de Ciências jurídicas, Universidade Federal de Santa Catarina, Florianópolis.

[23] CRESPO, Marcelo. **Revenge Porn. A Pornografia da vingança**, 2014. Disponível em: <http://marcelocrespo1.jusbrasil.com.br/artigos/153948423/revenge-porn-a-pornografia-da-vinganca> Acesso em maio.2020

contexto, condutas anteriormente inexistentes passam a exigir uma normatização como ocorreu no caso da *revenge porn.*[24]

De início, não havia no Brasil uma legislação específica prevendo o tratamento a ser dispensado nesses casos. Sendo assim, os casos eram enquadrados, nos crimes de difamação ou injúria, artigos 139 e 140, do Código Penal Brasileiro[25] resultando, na maioria das vezes, em penas restritivas de direitos como indenizações, o que gerava uma completa sensação de impunidade. Nos casos em que ocorria grave ameaça aplicava-se também o artigo 158 do Código Penal.

A depender da peculiaridade, outras legislações poderiam também ser aplicadas como o Estatuto da Criança e do Adolescente (Lei nº 8.069/90) no caso da vítima ser menor de idade e a Lei Maria da Penha (Lei nº 11.340/06) na circunstância em que existia um relacionamento íntimo entre a vítima e o responsável pela divulgação do conteúdo.[26] Isso porque a Lei Maria da Penha, em seu artigo 7º, incisos II e V, busca prevenir todas as formas de violência praticadas contra a mulher abarcando a violência física, psicológica e moral estando as duas últimas caracterizadas nos casos da pornografia de vingança. Bem como, os artigos 154-A e 154-B, ambos do Código Penal no caso do

[24] NUCCI, Amanda Ferreira de Souza; TEIXEIRA, Leonardo de Aquino. **Uma análise sobre revenge porn e a eficácia dos mecanismos jurídicos de repressão.** Revista Consultor Jurídico, 2019. Disponível em:<https://www.conjur.com.br/2019-jul-30/opiniao-revenge-porn-eficacia-mecanismos-repressao> Acesso em maio.2020.

[25] BUZZI, Vitória de Macedo. Pornografia de vingança: Contexto histórico-social e abordagem no Direito Brasileiro. 2015. 110 f. Monografia (Bacharelado em Direito) - Centro de Ciências jurídicas, Universidade Federal de Santa Catarina, Florianópolis.

[26] BUZZI, Vitória de Macedo. **Pornografia de vingança**: Contexto histórico-social e abordagem no Direito Brasileiro. 2015. 110 f. Monografia (Bacharelado em Direito) - Centro de Ciências jurídicas, Universidade Federal de Santa Catarina, Florianópolis.

material ter sido obtido por meio de invasão a dispositivos eletrônicos. E o Marco Civil da Internet (Lei nº 12.965/14) no que diz respeito ao direito da vítima em requisitar, diretamente aos provedores, a exclusão do material íntimo divulgado.

Contudo a Lei nº 13.718/18 consolida a crescente demanda social no que diz respeito a criminalização da pornografia de vingança[27] ao incluir um novo tipo penal previsto no artigo 218-C do Código Penal (citar o artigo), o qual busca coibir a divulgação de materiais que contenham de cena de estupro, estupro de vulnerável ou que faça apologia ou induza a sua prática; e de sexo, nudez ou pornografia sem o consentimento da vítima. O referido artigo ainda conta com um parágrafo, § 1º, o qual traz uma causa de aumento para situações em que o crime é praticado por agente que mantém ou tenha mantido relação íntima com a vítima com o fim de vingança ou humilhação[28], o qual se adequa perfeitamente à prática da pornografia de vingança. Visto que, os verbos do tipo aliados com as circunstâncias da causa de aumento descrevem a prática do *revenge porn*.[29]

Atualmente, tramitam na Câmara e no Senado projetos de lei que buscam combater essa violação à privacidade e intimidade da mulher, por exemplo, o Projeto de Lei n. 5.555/2013 que propõe

---

[27] BANQUERI, Poliana. **Nova lei representa avanço no combate à pornografia de vingança.** Revista Consultor Jurídico, 2018. Disponível em:<https://www.conjur.com.br/2018-out-01/poliana-banqueri-lei-avanco-pornografia-vinganca> Acesso em maio.2020.

[28] ARAUJO, Renan. Lei 13.718/18: **Alterações nos crimes contra a dignidade sexual. Importunação sexual, vingança pornográfica,** 2018. Disponível em: <https://www.estrategiaconcursos.com.br/blog/lei-13-718-18-alteracoes-nos-crimes-contra-a-dignidade-sexual-importunacao-sexual-vinganca-pornografica-e-mais/> Acesso em maio.2020.

[29] NUCCI, Amanda Ferreira de Souza; TEIXEIRA, Leonardo de Aquino. **Uma análise sobre revenge porn e a eficácia dos mecanismos jurídicos de repressão.** Revista Consultor Jurídico, 2019. Disponível em:<https://www.conjur.com.br/2019-jul-30/opiniao-revenge-porn-eficacia-mecanismos-repressao> Acesso em maio.2020.

uma alteração na Lei Maria da Penha para criar mecanismos para o combate a condutas ofensivas contra a mulher na internet ou em outros meios de propagação da informação.[30]

Conforme exposto, é perceptível que as discussões a respeito da pornografia de vingança sempre giraram em torno da necessidade de uma tipificação. Razão pela qual o legislador pátrio seguiu a tendência mundial ao criminalizar a referida conduta.[31] Reproduzindo todo o histórico do Direito Penal que é sempre voltado para o criminoso deixando a vítima de lado como se ela não fosse importante, e mais como se não ela não fosse um fator determinante para a concretização do fenômeno criminológico.

Dessa forma é importante que a vítima tenha o seu espaço ao longo do processo, pois só assim o judiciário seria capaz de conceder uma resposta satisfatória para ela, a vítima não pode ser apenas a pessoa que leva o fato ao conhecimento da autoridade policial e posteriormente é esquecida ao longo do processo penal, vindo aparecer novamente apenas em sede judicial para confirmar o depoimento prestado desconsiderando-se o sofrimento e a dor das mulheres vitimadas. Não apresentando, portanto, uma resposta suficiente ao problema.

Além do mais, muitas vezes o sistema acaba por duplicar a violência sofrida (vitória), pois as mulheres se sentem constrangidas pelo próprio Judiciário, desde seu depoimento na delegacia até a audiência de instrução. Tanto o é que atualmente

[30] BANQUERI, Poliana. **Nova lei representa avanço no combate à pornografia de vingança.** Revista Consultor Jurídico, 2018. Disponível em:<https://www.conjur.com.br/2018-out-01/poliana-banqueri-lei-avanco-pornografia-vinganca> Acesso em maio.2020.

[31] NUCCI, Amanda Ferreira de Souza; TEIXEIRA, Leonardo de Aquino. **Uma análise sobre revenge porn e a eficácia dos mecanismos jurídicos de repressão.** Revista Consultor Jurídico, 2019. Disponível em:<https://www.conjur.com.br/2019-jul-30/opiniao-revenge-porn-eficacia-mecanismos-repressao> Acesso em maio.2020.

busca-se cada vez mais criar delegacias especializadas com o objetivo de proporcionar um ambiente mais favorável e acolhedor a mulher vítima de violência.

Como a disseminação do conteúdo percorre o mundo de forma muita rápida, apesar de punir o homem, é muito difícil impedir a circulação do material pornográfico e quase impossível reparar os danos sofridos pela vítima. Primeiro porque o Direito Penal pátrio não consegue acompanhar a tecnologia e mesmo ao longo de um processo concede respostas muito tardias e pouco eficazes.

Segundo porque infelizmente, vivemos numa sociedade machista onde a nudez feminina remete a ideia de que a mulher é culpada do crime, por ter se permitido fotografar, filmar, usar uma roupa julgada socialmente como inadequada dentre outros, mesmo ela sendo a vítima. Então considera-se que a mulher foi merecedora do crime. No entanto, o homem, responsável pela divulgação, não é merecedor de reprimenda.[32] É a mulher que sofre retaliações sociais, profissionais e danos emocionais.

Dessa forma, apenas a normatização não é capaz de prevenir o crime e nem mesmo conceder uma resposta satisfatória para as vítimas, justamente porque as discussões são voltadas para a análise do crime a partir do criminoso, e não a partir do fenômeno criminológico com o olhar voltado para a vítima.

Sendo assim, o fenômeno da pornografia da vingança se apresenta como mais uma faceta da violência de gênero e que ganha ainda mais força com a culpabilização da vítima pela

[32] CRESPO, Marcelo. Revenge Porn. **A Pornografia da vingança,** 2014. Disponível em: <http://marcelocrespo1.jusbrasil.com.br/artigos/153948423/revenge-porn-a-pornografia-da-vinganca> Acesso em maio.2020.

sociedade o que só se justifica pelo histórico de dominação masculina que produz ou valida a pornografia da vingança.[33]

Nesse cenário, o sistema criminal também passa a dar mais importância pra relação autor-vítima envolvidos do que sobre o fato-crime cometido. A vítima busca o judiciário para julgar uma conduta mas acaba sendo ela mesma julgada. Logo, o sistema se mostra incapaz de proteger a mulher e, o castigo (pena), incapaz de cumprir com suas funções preventivas intimidatórias.[34]

Tendo em vista que as leis se prestam apenas a punir as condutas passadas, a preocupação principal deve ser impedir que as mulheres se tornem vítimas desse crime. Posto que, os danos causados à dignidade, à privacidade, à imagem e a honra da vítima podem ser irreversíveis devido ao rápido compartilhamento desses conteúdos.[35]

Por tudo isso, é que se faz necessário mudar o foco da discussão que é no réu e o objetivo que é punir para debater esse crime com um olhar sob a vítima. E questionar-se se a pena e a criminalização da conduta seriam a resposta ideal para vítima, pois para resposta ser eficaz seria necessário descobrir caminhos de prevenir o crime eliminando assim as dores e os danos causados à vítima.

---

[33] BUZZI, Vitória de Macedo. Pornografia de vingança: Contexto histórico-social e abordagem no Direito Brasileiro. 2015. 110 f. Monografia (Bacharelado em Direito) - Centro de Ciências jurídicas, Universidade Federal de Santa Catarina, Florianópolis.

[34] ANDRADE, Vera Regina Pereira de. **A soberania patriarcal: O sistema de justiça criminal no tratamento da violência sexual contra a mulh**er. Revista Sequência, 2005. Disponível em:<https://periodicos.ufsc.br/index.php/sequencia/article/view/15185>. Acesso em maio.2020

[35] CRESPO, Marcelo. **Revenge Porn. A Pornografia da vingança**, 2014. Disponível em: <http://marcelocrespo1.jusbrasil.com.br/artigos/153948423/revenge-porn-a-pornografia-da-vinganca> Acesso em maio.2020

1.3 Da vitimologia e prevenção vitimária

A vítima é fator determinante para a ocorrência do fenômeno criminológico. Não apenas a pessoa que leva o delito até a esfera criminal para ser julgado pelo juiz. A criminologia tem como finalidade o estudo do fenômeno criminológico exatamente no sentido explicitado considerando que para a ocorrência de um crime, vários fatores são determinantes. São eles: o crime, o infrator, a vítima e o controle social do comportamento delitivo. E é a partir da análise do estudo criminológico que aplica-se às estratégias mais eficazes para prevenir o crime.

A vitimologia é uma ciência autônoma que tem por objeto o estudo da vítima, sua relação com o criminoso e o impacto do crime em sua vida.[36] Logo, a vítima não pode ser interpretada como um fator passivo e estático do drama delitivo como se fosse irrelevante e não tivesse nada a acrescentar ou mesmo exigir ao longo do processo.

É de enorme relevância que a vítima apareça como sujeito ativo, tendo uma participação positiva e efetiva, que pode ser em maior ou menor grau, para a concretização do crime. Para que fosse respeitada e compreendida nos planos biológicos, psicológicos e social como a referida ciência prevê.[37] E segundo para que o Judiciário pudesse caminhar para obter a resposta mais eficaz e satisfatória para a própria vítima, pois muitas vezes a resposta almejada pela vítima se diverge da resposta perseguida pelo Estado que é a punição.

[36] VAZ, Paulo Junio Pereira. **Vitimologia e direitos humanos**.2013. Disponível em:<https://ambitojuridico.com.br/cadernos/direito-penal/vitimologia-e-direitos-humanos/> Acesso em maio.2020.
[37] Idem.

É importante para as ciências que estudam os delitos e suas consequências entender porque determinadas pessoas têm potencial para ser vítima e descobrir formas de tornar as experiências com os crimes menos traumáticas. Uma vez que a vitimologia e a proteção aos direitos humanos têm como objetivo o resgate ao respeito pelo ser humano e seus direitos fundamentais, buscando a mitigação dos danos sofridos pelas vítimas que tiveram seus direitos violados.[38]

A prevenção vitimária trabalha exatamente a possibilidade de prevenir o crime incidindo na conduta da vítima e assim impedir que ela crie um ambiente propício para a prática criminosa.

A ideia aqui explicitada é de considerar a vítima como um fator principal e primordial de análise e através disso construir respostas eficazes e medidas de prevenir o crime e seus efeitos. O intuito não é de culpar a vítima, porque ela não é culpada, nem de justificar um crime desmoralizando-a e nem mesmo de julgar ser ela merecedora da "*revenge porn*" como se faz na atual conjuntura. Posto que, a vitimologia foi concebida sobretudo para dar suporte às vítimas de todos os gêneros e compreendê-las.[39]

Portanto, a provocação trazida nesse artigo é que se busque cada vez alternativas suficientes para precaver a disseminação desse conteúdo e não para impedir a produção do material pornográfico ou de nudez. Uma vez que a mulher, vítima desse delito, é um ser autônomo e tem todo o direito de explorar sua sexualidade dentro ou fora de um relacionamento afetivo.

---

[38] Idem.

[39] VAZ, Paulo Junio Pereira. **Vitimologia e direitos humanos**.2013. Disponível em:<https://ambitojuridico.com.br/cadernos/direito-penal/vitimologia-e-direitos-humanos/> Acesso em maio.2020.

1.4 Dos caminhos para a prevenção

É salutar destacar que o ideal seria inibir a prática da divulgação desses materiais de cunho sexual através da educação geral, fortalecimento moral[40], mudança de uma visão machista impregnada na sociedade atual e na desconstrução da hierarquização dos sexos.

No entanto, alguns cuidados podem ser tomados para que o conteúdo seja enviado e a vítima mantenha alguma segurança. A *Coding Rights*[41] elaborou um guia elencando algumas dessas precauções, são elas:

1. Anonimato: é importante não mostrar o rosto, tatuagens, marcas de nascença, cicatrizes, móveis da casa e etc; alguns aplicativos como o Obscuracam pixalizam esses detalhes; e editores como o Photo Exif Editor apagam ou modificam os metadados[42].

2. Utilização de canais seguros: evite mandar nudes por SMS, *iMessage*, *Whatsapp*, *Telegram*, *Facebook*, *Tinder*, *Happn*, *Snapchat* ou qualquer outro aplicativo que mostre o número ou deixe o arquivo salvo. Aplicativos como *Confide* e *Wickr* permitem que as fotos se autodestruam imediatamente depois de vistas e caso ainda haja o print a pessoa será avisada. Além de permitirem cadastro sem associação do número de celular. É importante

[40] NUCCI, Amanda Ferreira de Souza; TEIXEIRA, Leonardo de Aquino. **Uma análise sobre revenge porn e a eficácia dos mecanismos jurídicos de repressão**. Revista Consultor Jurídico, 2019. Disponível em:<https://www.conjur.com.br/2019-jul-30/opiniao-revenge-porn-eficacia-mecanismos-repressao> Acesso em maio.2020.

[41] Codin Rights. Disponível em: <http://www.codingrights.org/wp-content/uploads/2015/11/zine_portugues_lado2.pdf> Acesso em maio.2020.

[42] São marcadores de dados de localização, horário, tipo de dispositivo e outras informações que servem para identificar a pessoa.

lembrar também de não associar a conta com o *Facebook* ou Gmail, pois os nudes seriam associadas a elas.

3. Usar senhas fortes e de preferência, longas, com caracteres e números. E não fornecer a ninguém;

4. Evitar utilizar conexões Wi-Fi compartilhadas em locais públicos para o envio dessas fotos;

5. Lembrar que toda foto enviada para um aplicativo é enviada para um servidor ao qual você não tem acesso, mas a empresa e o governo têm;

6. Deletar as fotos e ficar atento, pois o celular pode criar *backups*. Um aplicativo que ajuda a apagar os traços dos arquivos é o *Ccleaner*. Caso queira guardar as fotos é importante que seja em uma pasta criptografada.

Ressalta-se a importância do sigilo das senhas dos aplicativos, a qual não deve ser compartilhada nem mesmo ao longo do relacionamento íntimo, e se o for por um momento devem ser alteradas em seguida, além de ser indicado que as senhas dos aplicativos e dos dispositivos sejam diferentes, pois, caso alguma delas seja descoberta não permitirá o acesso a todos os aplicativos e dispositivos. Interessante também manter o cuidado com os links contaminados espalhados pela internet, pois alguns deles podem roubar arquivos que estão no seu celular e o antivírus atualizado.

Ao analisar também os fatores externos fora do alcance da vítima, outro caminho mais eficaz seria exigir dos grandes provedores uma atuação mais severa e efetiva quanto a divulgação desses materiais de cunho sexual mediante legislação. Visto que o atual amparo do Marco Civil da Internet possibilitou apenas a supressão desses conteúdos de forma rápida.

O Google e o Facebook, por exemplo, permitem a denúncia contra conteúdos impróprios e informam, ainda, ter uma equipe destinada para a análise dessas denúncias e remoção do conteúdo.[43] Não seria mais efetivo criar equipes para bloquear instantaneamente tais conteúdos? Esses provedores não poderiam criar barreiras de segurança que impedissem a postagem desse tipo de conteúdo? No caso dos sites pornográficos não se poderia exigir uma prévia identificação da pessoa para possibilitar apenas a postagem de conteúdo próprio?

Ante todo o exposto, é indiscutível que trata-se de um crime extremamente complexo cujos efeitos são imensuráveis e irreparáveis. Por isso, acredita-se ser mais adequado novas discussões a respeito do delito mantendo um olhar sob a vítima para evitar que o delito ocorra e caso ainda ocorra que a vítima possa ter no judiciário um ambiente que acolha e que a reafirme sua ausência de culpa.

Por fim, este artigo não se compromete a trazer o melhor caminho para a prevenção do *revenge porn*, mas tão somente indicar possíveis caminhos e assim incitar um debate importantíssimo que, ainda se faz necessário, apesar da tipificação da conduta.

2 CONCLUSÃO

O fenômeno da pornografia de vingança deve ser analisado sob a perspectiva da violência de gênero. Partindo-se da compreensão de que esse crime surgiu como o instrumento mais

[43] VARELLA, G; SOPRANA, P. **Pornografia de Vingança: crime rápido, trauma permanente** [online]. São Paulo, 16 Fev 2016. Fonte: Época. Disponível em: <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/02/pornografia-de-vinganca-crime-rapido-trauma-permanentee.html> Acessso em maio.2020.

atual de humilhar uma mulher publicamente, visto como mais uma forma de violência contra a mulher perpetrada pelos homens.

Nesse caminho, estabeleceram-se como objetivos específicos analisar a pornografia de vingança a partir da ótica da vítima e apresentar um caminho possível para diminuir os danos experimentados minimizando a incidência dos crimes.

Assim, em um primeiro momento objetivou-se traçar um panorama geral sobre o que consiste e como se originou a pornografia da vingança. Em seguida foi estabelecida a ligação dessa prática com todo o histórico, já conhecido, de violência contra a mulher. E por isso entendeu-se o crime como mais um instrumento capaz de perpetrar a violência de gênero.

Após, tratou-se de analisar como o ordenamento pátrio atuava nesses crimes tendo percebido que apesar de ser uma prática antiga apenas recentemente foi tipificado. E ainda sim continua sendo punido de uma forma não satisfatória ou suficiente, tendo em vista que apesar de ser atribuída uma pena mais severa ela não é capaz de prevenir o crime ou mesmo de minimizar seus efeitos.

No final, questionou-se a conduta dos provedores que mesmo tendo condições de evitar o crime, impedindo a divulgação dos conteúdos, se mantêm na posição de permitir a livre divulgação de tais conteúdos; e a ausência de uma legislação mais eficiente que obrigasse as empresas dos provedores e aplicativos a impor uma política mais severa aos usuários.

Então conclui-se ser necessário evitar a prática desse crime influindo na conduta da vítima e não do criminoso. Nesse contexto, a opção da prevenção ganhou destaque e logo depois, foi apresentado um caminho capaz de tornar o envio dos materiais

sexuais e pornográficos mais seguro. Para que tais materiais não tenham o condão de prejudicar essas mulheres após o fim do relacionamento.

REFERÊNCIAS

ANDRADE, Vera Regina Pereira de. A soberania patriarcal: O sistema de justiça criminal no tratamento da violência sexual contra a mulher. Revista Sequência, 2005. Disponível em:<https://periodicos.ufsc.br/index.php/sequencia/article/view/15185>. Acesso em maio.2020.

ARAUJO, Renan. Lei 13.718/18: Alterações nos crimes contra a dignidade sexual. Importunação sexual, vingança pornográfica, 2018. Disponível em: <https://www.estrategiaconcursos.com.br/blog/lei-13-718-18-alteracoes-nos-crimes-contra-a-dignidade-sexual-importunacao-sexual-vinganca-pornografica-e-mais/>. Acesso em maio.2020.

BANQUERI, Poliana.Nova lei representa avanço no combate à pornigrafia de vingança. Revista Consultor Jurídico, 2018. Disponível em:<https://www.conjur.com.br/2018-out-01/poliana-banqueri-lei-avanco-pornografia-vinganca> Acesso em maio.2020.

BUZZI, Vitória de Macedo. Pornografia de vingança: Contexto histórico-social e abordagem no Direito Brasileiro. 2015. 110 f. Monografia (Bacharelado em Direito) - Centro de Ciências jurídicas, Universidade Federal de Santa Catarina, Florianópolis.

Coding Rights. Disponível em:<http://www.codingrights.org/wp-content/uploads/2015/11/zine_portugues_lado2.pdf> Acesso em maio.2020

CRESPO, Marcelo. Revenge Porn. A Pornografia da vingança, 2014. Disponível em <http://marcelocrespo1.jusbrasil.com.br/artigos/153948423/revenge-porn-a-pornografia-da-vinganca> Acesso em maio.2020.

DAILY.2010. Disponível em: <http://www.dailymail.co.uk/news/article-1329812/Joshua-Ashby-Facebook-user-jailedposting-naked-picture-ex-girlfriend.html> Acesso em maio 2020. Disponível em: <http://www.endrevengeporn.org/main_2013/wpcontent/uploads/2014/12/RPStatistics.pdf> Acesso em maio 2020

KHOURI, José Naaman. Violência contra a mulher. MidiaNews, 14 de fevereiro de 2012. Disponível em: <http://www.midianews.com.br/conteudo.php?sid=262&cid=81369>. Acesso em maio.2020.

NUCCI, Amanda Ferreira de Souza; TEIXEIRA, Leonardo de Aquino. Uma análise sobre revenge porn e a eficácia dos mecanismos jurídicos de repressão. Revista Consultor Jurídico, 2019. Disponível em:<https://www.conjur.com.br/2019-jul-30/opiniao-revenge-porn-eficacia-mecanismos-repressao> Acesso em maio.2020.

VARELLA, G; SOPRANA, P. Pornografia de Vingança: crime rápido, trauma permanente [online]. São Paulo, 16 Fev 2016. Fonte: Época. Disponível em: <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/02/pornografia-de-vinganca-crime-rapido-trauma-permanentee.html> Acesso em maio.2020.

VAZ, Paulo Junio Pereira. Vitimologia e direitos humanos.2013. Disponível em:<https://ambitojuridico.com.br/cadernos/direito-penal/vitimologia-e-direitos-humanos/> Acesso em maio.2020.

WINKLEY; Lyndsay; LITTLEFIELD, Dana. Sentence revised for revenge porn site operator. postado em 21 set. 2015. Disponível em <https://www.sandiegouniontribune.com/sdut-kevin-bollaert-revenge-porn-case-resentencing-2015sep21-story.html> Acesso em maio.2020.